MailBox X.400

MessageGate for OpenMS V5.1

User's Guide

V1.8

All products or services mentioned in this document are identified by the trademarks or registered trademarks of their respective companies or organizations. Telekom Deutschland GmbH claims no responsibility for specifying which trademarks are owned by which companies or organizations.

The information in this guide is subject to change without notice. The information does not represent a commitment on the part of Telekom Deutschland GmbH. Telekom Deutschland GmbH is not responsible for any errors that may appear in this manual. It is illegal to copy this document except with specific permission in a license or non-disclosure agreement. The manual or parts of the manual may not be reproduced or transmitted in any form or by any means, electronically or mechanically, including photocopying and recording, for any purpose, without the express written permission of Telekom Deutschland GmbH. No parts of this publication may be transcribed, stored in a retrieval system or translated into any language without the prior written consent of Telekom Deutschland GmbH.

Copyright © 2015

Telekom Deutschland GmbH

BusinessMail X.400

Postfach 107300

68165 Mannheim

Index

0 PREFACE 1

0.1 Please send any comments to the following E-mail address 1
0.2 The following conventions are used in this guide 1
0.3 The following abbreviations are used in this guide 2
0.4 New in V1.8 3

1 INTRODUCTION TO MESSAGEGATE FILE INTERFACE 4

1.1 With MessageGate File Interface you can: 4
1.2 X.400 – an International Standard 4
1.3 The motives in implementing MessageGate 4

2 INTERFACE DESCRIPTION 6

2.1 Overview 6
2.2 MessageGate User's directory 11
2.3 The Message file 13
2.3.1 The Message Header 13
2.3.2 Address format 15
2.3.3 Message Content 17
2.4 The Forwarding of a message is not supported 20
2.5 Transmission Set File Format 21
2.5.1 The central EDI function 21
2.5.2 The Content of Transmission Set Files 22
2.6 The Status Report 23
2.6.1 General 23
2.6.2 Request a Status Report 23
2.6.3 Status Report Syntax (readable structure) 25
2.6.4 Syntax of Status reports (CSV structure) 30
2.7 Send Receipt Notification 31
2.8 Communication and Trading Relation Profile 32
2.8.1 General 32
2.8.2 X.400 Reports 33
2.8.3 X.400 Header Information 34
2.8.4 X.400 Body parts 35
2.8.5 Encoding of binary data 35
2.8.6 File format (Format of output) 35
2.8.7 Request Status Report in WebConfig 35
2.8.8 Configure automatically generated Status Report 36
2.8.9 EDI Relation 36
2.8.10 SMTP Filter 37

3 ACCESS VIA SFTP (SSH) 40

3.1 General 40
3.2 Features to note 40
3.3 Recommended SFTP Communication modules 41
3.3.1 Using Microsoft® Windows 32 Bit Operating systems: 41

3.3.2 Microsoft® Windows 64 Bit Operating systems 47
3.3.3 Linux and UNIX Operating system 47
3.3.4 Apple Mac OS X 48
3.3.5 Other operating systems 48

4 ACCESS VIA HTTPS/WEBDAV 50

4.1 General 50

4.2 Features to note 51

4.3 Recommended WebDAV Clients 51

4.3.1 Microsoft® Windows 32 Bit Operating systems 51
4.3.2 Microsoft® Windows 64 Bit Operating systems 58
4.3.3 Linux and UNIX Operating system: 58
4.3.4 Apple iOS 59
4.3.5 Other operating systems 61

5 AS2 AND MESSAGEGATE PROCESS 62

5.1 General 62

5.2 Differences between File Interface and AS2 users 64

6 OFTP AND MESSAGEGATE 72

6.1 General 72

6.2 Differences between File Interface and OFTP Users 74

7 SMTP MTA AND MESSAGEGATE 88

7.1 General 88

7.2 Difference between File Interface and SMTP MTA users 88

8 IMPLEMENTATION OF MESSAGEGATE SOLUTION 94

8.1 Using Standard E-Mail Clients 94

9.1.1 Using Outlook Express 94
9.1.2 Using Mozilla Thunderbird 94

8.2 Designing a MessageGate solution 95

8.3 Open Source Client for MessageGate 95

APPENDIX A X.400 ADDRESS ELEMENTS 100

APPENDIX B: ERROR CODES 102

B1. Error codes of MessageGate Poller process: 102

B2. MessageGate Error codes 103

B3. MTA Error codes (Non Delivery Notification) 110

Error codes in NDN: 110
Reason codes in NDN 111

B4. X.400 User Agent Error codes (Non Receipt Notification) 118

Error codes in NRN: 118
Reason to discard messages: 118

B5. Mapping rules NDN to DSN 119

APPENDIX C: EXAMPLES FOR MESSAGES AND REPORTS 122

C1. Delivered Message with text attachment 122

C2. Delivered Message with binary attachment 122
C3. Delivered Message with Multiple attachments 123
C4. Delivered Message with Multirecipient 123
C5. Submitted Message and no Report Request 124
C6. Submitted Message with Report Request 125
C7. Submitted Message with Multirecipient 126
C8. Transmission set with two Interchanges 127
C9. Status Report without History 128
C10. Status Report with History 130
C11. Status Report for a selected Order-ID 131
C12. Status Report for a selected Message-ID 132
C13. Status Report for denied Messages 132
C14. Report for submitted message (Multirecipient) 133
APPENDIX D: CHARACTER SETS 136

0 Preface

The Product

This guide contains information about MessageGate, a file interface to the *BusinessMail X.400* MailBox service, to send and receive messages based on the ITU/ISO X.400 standard.

The Customer

This new interface will help those customers, who do not have the possibility of using a standard X.400 Mail client (a so called P7 Remote User Agent) for communicating with X.400 partners. MessageGate is available in addition to the existing Batch User Agent (BUA) file interface, which it will replace in the long term.

Additional Documents

- See also Batch User Agent Reference Guide
- RFC822, RFC1521

Registered trademarks

Microsoft® and WindowsTM are trademarks of the Microsoft Corporation. Other product and company names that are mentioned in this manual are included to identify the products. They may be trademarks or registered trademarks for the companies they belong to.

0.1 Please send any comments to the following E-mail address

businessmail.help@telekom.de, Subject: MessageGate User Guide

0.2 The following conventions are used in this guide

This typeface	Indicates contents of messages/headers submitted over the MessageGate file interface
This typeface	Indicates MessageGate interface parameters, elements or values

0.3 The following abbreviations are used in this guide

API	Application Programming Interface
AS2	Applicability Statement 2 - Standard (EDIINT) for B2B communication via Internet (RFC 4130)
BUA	Batch User Agent – File Interface of *BusinessMail X.400* MailBox service accessing a customer's mailbox
BP14	Bodypart 14 – Bilaterally defined (binary) CCITT X.400 Standards (1984)
CSV	comma-separated values - a simple text format for a database table where record in the table is one line of text file
CUG	Closed User Group
DDA	Domain Defined Attributes (X.400 address elements)
DN / NDN	X.400 Delivery Notification (report) or Non Delivery Notification (report) generated by X.400 MTA
EDI	Electronic Data Interchange, a particular set of standards for computer-to-computer exchange of information
EDIFACT	Standard for Electronic Data Interchange – ISO 9735
EERP	OFTP EERP (End-to-End Response)
FTBP	FTAM (FileTransfer, Access and Management) body part, used to transfer binary content including file information (eg.file name, type of content etc.).
FTP	File Transfer Protocol (RFC 959)
ILN	International Location Number (registered EDI address)
GDI	Global Domain Identifier (X.400 Terminology)
GLN	Global Location Number (registered EDI address)
MB	Megabyte – 1 000 000 bytes – definition recommended by the International System of Units (SI)
MDN	Message Disposition Notification – Report type used for SMTP (RFC 3798) and AS2 (RFC 4130)
MIME	Multipurpose Internet Mail Extensions (RFC 2045, RFC 2046, RFC 2047, RFC 4288, RFC 4289 and RFC 2049)
MPLS	Multi Protocol Layer Switching – IP Backbone using a labeling mechanism to implement a VPN
MS	(X.400) Message Store
MTA	(X.400) Message Transfer Agent
NERP	OFTP NERP (Negativ End Response)
OFTP	Odette File Transfer Protokoll
P2 / P22 / P35	X.400 message types
P7	X.400 protocol standard describing how an X.400 Client communicates with a MS (Message Store)
PEDI	Special X.400 EDI message type defined in X.435 (equivalent to

	P35)
RFC	Request for Comment – Internet Standards Track
RN / NRN	X.400 Receipt Notification (report) or Non Receipt Notification (report) generated by X.400 user agent (client)
SFTP	Secure File Transfer Protocol (Part of the Secure Shell Protocol suite, RFC 4259 ff)
SMTP	Simple Mail Transfer Protocol – Internet Mail Protocol Standard (RFC 822 ff)
SMS	Short Message Service – Send SMS via *BusinessMail X.400* SMS Gateway
TS	Transmission Set (EDIFACT) – a file containing a sequence of Interchanges
UNB	EDIFACT Interchange Header
UNZ	EDIFACT Interchange Trailer
VDSN	Virtual Data Set Name (RFC 5024 = SFIDDSN = Virtual File Dataset Name)
VPN	Virtual Private Network
WebDAV	HTTP Extensions for Distributed Authoring (RFC 2518) – increases the command set of http (copy, move)
WebConfig	*BusinessMail X.400* management configuration platform, with which a customer can configure his environment and his partnerships (aka. relations)

0.4 New in V1.8

- Chapter “OFTP and MessageGate Process” has been added.

1 Introduction to MessageGate File Interface

1.1 With MessageGate File Interface you can:

- Send messages to other *MailBox X.400* users, to partners on other X.400 systems and to Internet mail users. MessageGate supports both the 1984 and 1988/92 X.400 Standards.
- Send messages to Fax or SMS recipients.
- Check the status of your messages and import the results into your application.
- Create a Receipt Report for a message that you have received in your application.
- Use standard mechanism of the TCP/IP protocol suite (SFTP, https with WebDAV extension) to upload messages/data to the MailBox service or to download received messages/data.

1.2 X.400 – an International Standard

X.400 is the name of an International standard (ITU, ISO) for the exchange of electronic messages. It specifies the requirements and recommendations of programs used for electronic mail. It includes specifications how a message is to be addressed, which characters are allowed and how communication is to take place.

The X.400 standard defines Delivery Reports/ Notifications and also Receipt Reports/ Notifications, in order to track the status of a submitted message.

Around the world there are many telecommunication networks which provide services enabling messages to be exchanged in accordance to the X.400 standard. One of X.400 greatest advantages is that it enables the exchange of messages with users working with different types of computers using secure networks.

1.3 The motives in implementing MessageGate

BusinessMail X.400 has over several years provided a file interface called Batch User Agent (BUA) for host server communication. With the BUA a customer specific directory is provided on the MailBox service server environment where a customer can use FTP to upload/download data and command/result files.

Using the BUA a customer defines in his command file the message data and the recipients to which it should be sent and whether message data should be fetched from his message store (mailbox polling). The user data of the downloaded messages is stored in his customer specific subdirectory and the header information is provided in a result file. The customer can download his user data and the result file via FTP and process these in his application. This interface has stood the test of time but the syntax used with this interface is not trivial so the development of customer applications can be expensive.

During the development of an AS2 Gateway for *BusinessMail X.400* a new interface was designed for customers who used this new communication access method but still needed to communicate with their existing X.400 partners. This new file interface, now called MessageGate File Interface (in the document often referred to as MessageGate), is also available to customers that use https with WebDAV extension or SFTP to upload and download messages and data. The new Message-Gate file interface has the following advantages:

- SMTP/MIME compatible syntax
- Messages are delivered directly to the customer's specific directory so the polling of the customer's Message Store, as is done with the BUA, is not necessary

There are a lot of tools and libraries available in the public domain supporting the SMTP/MIME syntax. Hence the cost and complexity of developing applications that use the new MessageGate interface to send and fetch X.400 messages should be a lot less in comparison to the existing BUA interface. MessageGate conforms to RFC822 and RFC 1521 and all other MIME relevant RFC.

2 Interface Description

2.1 Overview

This Chapter gives a short description of all MessageGate File Interface functions. More details of each of the MessageGate functions can be found in subsequent Chapters in this manual. Examples of messages and reports and also a list of all error codes can be found in the Appendix.

A working directory is configured on the *BusinessMail X.400* application servers for each MessageGate user. A MessageGate user has to decide whether to use SFTP or https with WebDAV extension to upload/download messages. The filename extension defines how the data will be processed (".IN" → defines data that is to be sent, ".OUT" → defines data that has been delivered by MessageGate).

As the MessageGate process cannot verify in all cases when an uploaded file has been transferred completely, a file that is being uploaded should initially use the file extension ".TMP". When the file upload is finished the file extension should then be renamed by the sending application to "*.IN". The MessageGate process uses a similar mechanism when delivering messages to the customer specific directory, whereby these temporary files are kept invisible to the MessageGate user.

Please note that the term Order-ID used in the following sections is not to be confused with any EDI terminology, but just implies a processing related reference number.

Submit a message

Step 1: Client → Upload the file "M_Order-id.tmp" using https/WebDAV or SFTP to MessageGate directory

Step 2: Client → Rename the file "M_Order-id.tmp" using https/WebDAV or SFTP to "M_Order-id.IN"

Step 3: MessageGate processes the file "M_Order-id.IN", submits an X.400 message and deletes this file

Deliver a message

Step 1: MessageGate fetches a message out of the X.400 MTA queue and stores this message in file "M_Order-id.OUT" in the MessageGate user's directory

Step 2: Client → Download the file "M_Order-id.OUT" using https/WebDAV or SFTP and deletes this file in the MessageGate user's directory.

MessageGate will process all files starting with "M_" as messages. The Order-ID should not be longer than 22 characters. Only integer numbers, the letters A-Z or a-z and a few special characters ("_", "-", "$") are valid for the field Order-ID. **Please refer to the information regarding file version numbers in the next Chapter in this manual.**

MessageGate processes a message file that includes header information (sender, recipient, subject, Message-ID …) and content (one or multiple attachments) in SMTP/MIME (Version 1.0) format. MessageGate will not accept messages with an empty content. You may add a list of up to 50 recipients (tested) for each message. The restriction that mailbox users can only address one MessageGate user has been dropped.

Example of a message that illustrates the syntax of a delivered (i.e. to a MessageGate user) message that has multiple attachments
Name: M _5K00AG0HBDM0F2F8.OUT

To: "G=MG1;S=MGATE;CN=MG1 MGATE;O=TEST;A=VIAT;C=DE" <49603@viaT.de>
From: "G=ipm;S=tester;O=test;A=viaT;C=de" <21046@viaT.de>

```
Message-ID: 614 07/11/13
X-MPDUID: 8B0663A011DCEC4417009682
Date: 13 Nov 2010 13:10:22 +0100
Subject: Test with 3 Body parts
Disposition-Notification-To: "G=ipm;S=tester;O=test;A=viaT;C=de"
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="MG_=_CA610D0211DC91E900007CAD_=_MG"


--MG_=_CA610D0211DC91E900007CAD_=_MG
Content-Type: text/plain
Content-Transfer-Encoding: 8bit

Test äöüÄÖÜß

--MG_=_CA610D0211DC91E900007CAD_=_MG
Content-Type: application/octet-stream
Content-Disposition: attachment; filename="4d654d1d.zip"
Content-Transfer-Encoding: binary

PK□□□  □ tYr2ÄQa6÷□ ‹□4d654d1d.0µ“ls£:□…÷Tñ¨ê¥Ói3xJU/$!¦DØb2xgd□°1Ø
.
    □ ¶□  4d654d1d.0PK□□  □ □ 8 □
--MG_=_CA610D0211DC91E900007CAD_=_MG
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from url=(0062)https://securep7.viat-test.de/~0000001045/result/fetch_all.RES -->
<HTML><HEAD>
<META http-equiv=Content-Type content="text/html; charset=windows-1252">
<META content="MSHTML 5.50.4930.1700" name=GENERATOR></HEAD>
<BODY><XMP>LOGIN::
.
</XMP></BODY></HTML>
□
--MG_=_CA610D0211DC91E900007CAD_=_MG—
```

Rules when sending messages

Mandatory message elements are: “To:” and Content-Type/Encoding. All other message elements are optional. If the Message-ID is not defined MessageGate will use the Order ID instead to map this to the X.400 Message-ID.

The addresses used for “To:”, “Cc:”, “Bcc:” and “From:” (Mixture of small and capital letters possible) have an Alias part where the X.400 address (elements separated by semicolon “;”) might be defined and a RFC822 address part (<x@viat.de> or <User-id@viat.de>):

Possible address forms:

1. “c=de;a=viat;P=prmd;o=org;s=Surname;g=Given name“ <x@viat.de>

   External address without User-ID

2. ““ <73237@viat.de>

   Local or external address with User-ID

3. “ c=de;a=viat;o=org;s=Surname;g=Given name“ <71111@viat.de>

   Address, MessageGate will use when delivering a message and the User-ID of the sender is available

When sending a message using the third address form for “To:”, “Cc:” or “Bcc:” MessageGate will use the X.400 address elements and will not verify the defined User-ID.

If the central EDI function is activated for a MessageGate user it is also possible to upload one or several EDIFACT interchanges while using a Transmission set file to

send this data to partners or to download a file that includes such an EDIFACT interchange without any other header information.

Examples of Transmission set file
Name: T_5K00AG0HBDM0F2F8.OUT

```
UNA:+.? '
UNB+UNOA:2+MGATE1:65+TESTER:65+020508:1413+0709210008'
UNH+EVA0000001+INVOIC:D:95A:UN:ETEIB++0'
.
.
UNT+37+EVA0000001'
UNZ+1+0709210008'
```

To minimize the number of required elements in the header of SMTP/MIME messages the mapping rules to create an X.400 message (message type, mapping of MIME body parts into X.400 body parts, request for report etc) can be defined in so called Host based profiles (user profile, partner profile). It is not necessary to set up a host profile for each partner. MessageGate will use the parameters defined in the user profile if it does not find a partner profile. Defining a partner profile is only necessary if the required communication parameters differ from the default parameters (for example different message type or different report type).

Parameters in user profile or partner profile

- Mapping request for report in SMTP header (Disposition-Notification-To:) in X.400 request for Non Delivery Notification (NDN), Delivery Notification (DN) or Receipt Notification (RN) when sending messages (Default is DN)
- Mapping of Receipt Notification into “Disposition-Notification-To:” for delivered messages (Default is to map)
- Expiry time of X.400 message in minutes (Default is 1440 -> 24 hours)
- Type of X.400 message (Default is IPM88) while sending the X.400 message
- Mapping of MIME body into X.400 body part (Default is Variable -> Mapping into correspondent bodypart) while sending (similar rules apply for the opposite direction) the X.400 message (similar rules apply for the opposite direction)
- Deliver binary MIME body in content encoding “BASE64“ or ”Binary“ (Default is Binary)
- Deliver EDIFACT Documents in Transmission Set file or in SMTP syntax file (only available when central EDI Function is activated und only available in user profile -> Default is Transmission Set file)

MessageGate will not deliver X.400 reports in the user directory. Information about the status of submitted messages may be requested via status reports. A status report can be requested manually via the interface or delivered automatically (parameter setting in User profile).

Example for request of status report
Name: S_040308001.IN

Format: History
Direction: both

Parameters valid for request of status report (logical “and” notification)

Disposition:	All, Modified (Default is All, all entries, not only those that have changed since the last request)
Direction:	Sent, Received, Both (Default is Sent)
Format :	History, CSV-C, CSV-S, Actual (Actual -> Status of messages and not all status changes)
Message-ID:	Message number or only a part of it
Order-ID:	Order number or part of it
Since:	dd-mmm-yyyy hh:mm:ss, since date: day, month, year, hours, minutes, seconds

MessageGate will store the requested status report in a structured file. Hence it is possible to import this information about the submitted and received messages and the corresponding reports into the customer’s application. When sending a message to more then one recipient the status report will contain an entry for each recipient. In this case the Message-ID and Order ID will only be unambiguous in conjunction with a specific recipient address. When receiving messages there is still one entry displaying the originator’s address. The complete recipient list is available in the MIME header of the message file.

Example of a status report entry with parameter Format set to “Actual” (S_Order-ID.OUT)
Status Report for UserID 49603; generated 13-NOV-2010 14:56:23
Filters: Disposition=All, Direction=Both, Format=Actual, Since=13-Nov-2010

From: " G=ipm;S=tester;O=test;A=viaT;C=de" 21046@viaT.de
Order-ID: 5K00AG0HBDM0F2F8
Message-ID: 614 10/11/13
MTS-ID: CA610D0211DC91E900007CAD
Status: Read
Date: 13-Nov-2010 14:01:18 +0100

Example of a status report entry with parameter Format set to “History” (S_Order-ID.OUT)
Status Report for UserID 49603; generated 13-NOV-2010 14:56:22
Filters: Disposition=All, Direction=Both, Format=History

To: "" 21046@viaT.de
Order-ID: Test_3_Body011
Message-ID: 260002 12/11/10 MGATE Test
MTS-ID: 098FC66111DC91F80000A6BD
Sent: 13-Nov-2010 14:52:21 +0100
Delivered: 13-Nov-2010 14:52:27 +0100
Read: 13-Nov-2010 14:54:00 +0100

Status report entries where the parameter Format is set to “Actual” will always have a length of 6 lines. If the parameter Format is set to “History” the numbers of lines is variable (5-7) depending on the message status.

As an alternative to the readable reports output format a report with the format “CSV-S” (CSV format separated by semicolon) or “CSV-C” (CSV format separated by co-lon), that is optimized for automatic processing, can be selected.

In Chapter 2.8 Communication and Trading Relation Profile detailed information is available of how to configure the automatic delivery of status reports to the file inter-face.

Based on a bilateral agreement with your X.400 partner and assuming that the partner has requested this in his message a receipt notification for a delivered message can be generated:

Example of sending a Receipt Notification
Name: R_5K00AG0HBDM0F2F8.IN

Possible Values are:

Processed	→	Receipt Report/Notification (RN)
Failed	→	Non Receipt Report/Notification (NRN)

The MessageGate process will delete all the processed files ("*.IN") in the user's directory. All other files (delivered messages, status reports or any other kind of files uploaded to this directory) which are stored in the user's directory, will be deleted by a "Purger" process after a predefined lifetime. The *BusinessMail X.400* support team will configure this "lifetime" for each customer individually. It is our recommendation that the customer's application proactively deletes all downloaded files to reduce the number of files stored in the user's directory.

A "Purger" process also exists to process the database relation (Trace_Tab) where all messages/transactions status information is stored. The *BusinessMail X.400* support team will configure the "lifetime" of these entries (Default is 240 hours) for each customer individually.

The "MessageGate" process will handle two classes of processing errors. It will check the syntax and the completeness of message files in the user's directory and will stop processing the content if there is an error. The message file will remain in the user's directory and the file name will be extended by an error code (see Appendix B). MessageGate will also add an entry in the database so that the problem is reflected in the status report. Similarly when the "MessageGate" process experiences an error whilst sending a message via the X.400 MTA, it will add this error code to the respective entry in the database/status report.

It is also possible to subscribe to a MessageGate mailbox that has reduced functionality. In such a case the user can only receive messages. The transmission of messages or receipt notifications is not possible, nor the manual request of status reports. The automatic delivery of status reports, configured via *WebConfig*, is still possible.

Using the central EDI function in combination with the reduced MessageGate mailbox functionality described above, it would be feasible to use a Web browser to download the data (EDIFACT documents) and feed this into an application.

2.2 MessageGate User's directory

The MessageGate process does not require any sub directories in the user's directory. Only the file extension defines if a message should be sent ("*.IN") or if a message has been delivered ("*.OUT") to the user's directory.

The MessageGate process delivers all messages to the user's directory immediately after having processed these from the X.400 MTA queue.

The "Poller" process also frequently checks if there are files in the user's directory to process ("*.IN"→ send messages or Transmission Sets, send Status report and send Receipt Notifications). The scheduling of this check is defined on a user group basis. At the present time only one user group has been defined (schedule interval: 1 minute).

When the "Poller" process finds files with the file extension "*.IN", it tries to process these files immediately. However the "Poller" process is not always able to verify that a file has been uploaded completely.

Therefore a file should be always uploaded using the ".TMP" file extension. The file should then only be renamed to "*.IN" once the upload has completed.

Please consider that the actual configuration of the OpenVMS Operating System on which Message Gate's application server is running on, will only accept one dot (".") in the filename. The part of the filename following the dot is known as the file extension.

The first character of the filename defines the type of file (message, report/report request, receipt report request). The next character, an underscore "_", separates the Order ID which can have a maximum length of 22 characters.

Only integer numbers, the letters A-Z or a-z and the following special characters are valid for this Order ID:

Hyphen "-"

Underscore "_"

Dollar sign "$ "

The Order-ID as well as the Message-ID must be unique otherwise MessageGate cannot update the transaction log data (Trace_Tab) in the database when receiving reports. Please consider that the OpenVMS Operating System on which Message Gate's application server is running on stores files using version numbers. That means that the files with same file name will not be replaced, but will be stored with different version numbers. When accessing the directory via https/WebDAV this behavior is not visible. When accessing a file (open, delete etc.), the file with the highest version number will always be used. In the case where multiple files with the same file name are present, if a file is deleted, then the older file (with the preceding version number) will become visible in the directory.

MessageGate uses the following file naming convention:

a) Message with header file for sending:
M_<Order-ID>.IN

b) Transmission Set file (one or several Interchanges) without header for sending:
T_<Order-ID>.IN

c) Receipt report file for sending:
R_<Order-ID>.IN

d) Status report file request:
S_<Order-ID>.IN

e) Delivered message file with header:
M_<Order-ID>.OUT

f) Delivered Transmission Set file (one Interchange) without header:
T_<Order-ID>.OUT

g) Delivered Status report file:
S_<Order-ID>.OUT

Capital and small letters for the file name and extension can be used, but please note that the filter mechanism (parameter Order-ID) in status requests is case sensitive.

Please refer to later Chapters in this document to find more details regarding the format of these files.

If the MessageGate “Poller” process discovers a problem in message files (Syntax error, file is incomplete etc.) the file will remain in the directory but the name of the file will be extended with the respective error code (for example M_12345.in_ERR0005, if the file was not uploaded completely).

2.3 The Message file

The message file includes header and content (MIME content). The syntax of the content conforms to RFC1521 and subsequent RFC. The header of a message file is based on RFC822 (SMTP) and includes information that MessageGate as well as the recipient requires to handle/process the content. MessageGate uses only those header elements which are necessary to build the X.400 message. All other header elements will be ignored.

To minimize the number of header elements the required X.400 message parameters are stored in host profiles (user and partnership profiles)

The content part of the message file may contain a single or several document/ body (multipart). The MIME content type has to be defined in the header information. MessageGate does not accept messages with empty content,

The maximum message size may not exceed 100 MByte. When sending messages up to 50 recipients (tested) can be added, but there must be at least one “To:” recipient in the message. In delivered message all recipients are present in the MIME header.

2.3.1 The Message Header

MessageGate uses the following header elements to create X.400 messages or to deliver X.400 messages to the MessageGate file interface. MessageGate differentiates between mandatory and optional header elements during the sending of messages (“*.IN”). MessageGate provides all header elements when delivering message files (“*.OUT”).

From:

Message originator: optional (for format rules: see next Chapter), if used, the address has to be valid!

To:

Message recipient: mandatory (for format rules see next Chapter)

At least one “To:” recipient has to be added to the MIME header.

Cc:

Message copy recipient: optional (for format rules see next Chapter)

Bcc:

Message blind copy recipient: optional (for format rules see next Chapter)

Message-ID:

Message-ID that is also used for the X.400 Message-ID when sending the X.400 message or mapped from the X.400 Message-ID in delivered messages, optional

Maximum length is 64 characters of printable string character set. Please ensure that this Message-ID is unique so that the message recipient has no problems processing the message and so that MessageGate is able to update the transaction log in the database.

If the MessageGate process does not find a Message-ID in the header of the message it will map the Order ID to the X.400 Message ID.

Please be aware that the *BusinessMail X.400* Fax Gateway only supports a Message-ID with a maximum length of 16 characters. When a longer Message-ID is used the Message-ID visible on the fax document will be truncated.

Subject:

The subject element is mapped when sending an X.400 message and will be mapped from an X.400 message subject field when delivering a message to the file interface, optional.

The maximum length of the subject element is 128 characters (Teletex character set T.61).

Please be aware that the "MessageGate" process will <u>not</u> convert German characters (ä,ö.ü,Ä,Ö,Ü,ß) in the X.400 message subject field when delivering a message (ie. against the conventions of RFC822). In addition to accepting this format for messages destined for transmission, MessageGate will also accept messages with the standard encoding (ISO8859-1 character set → "=?iso-8859-1?x?...txt...?=" where x=Q → quoted-printable or x=B → Base64).

Date:

Date of message (Date and Time Specification of RFC 822): optional
MessageGate will not use this date in an X.400 message.

Examples of the format:

2 Nov 2010 09:31:44 +0100 (Format of delivered message, English abbreviation of month)

Tue, 2 Nov 2010 09:31:44

Disposition-Notification-To:

Request a report: optional.
This request will be mapped to an X.400 report request based on the Host profile parameter "When sending X.400 Messages map a requested Notification into":

0 → Requests Non Delivery Notification (NDN)

1 → Requests Delivery Notification (DN)

2 → Requests Receipt and Delivery Notification (RN and DN)

For more information see Chapter 2.8.2 X.400 Reports.

MessageGate will map this MIME header element to a delivered message if a receipt notification was requested by the sender in the X.400 message and if this RN is not suppressed in the profile. The customer's application may send a receipt notification (see Chapter 2.7 Send Receipt Notification).

In a delivered message MessageGate will write the X.400 address of the originator within quotation marks after of the key words of the element "Disposition-Notification-To:". When sending a message it is not necessary to add a value within quotation marks because MessageGate will ignore this information.

Examples:
Disposition-Notification-To: "" (when sending messages)

Disposition-Notification-To: "c=de, a=viat; s=tester; o=test" (delivered message)

X-MPDUID:

Message number allocated by the X.400 MTA when a message has been submitted (only used in delivered messages), maximum 32 characters (the MPDU ID of a submitted message will be displayed in the status report parameter MTS-ID)

MIME-Version:

Optional: Default: 1.0 (only this version will be supported).

Content-Type:

Type of MIME data (RFC 1521 “Multipurpose Internet Mail Extensions“ and subsequent RFC), **mandatory**.

This parameter defines the content type of a message. This has to be present after the header elements and only in combination with the elements “Content-Transfer-Encoding: “ and if necessary “Content-Disposition:“. The actual content follows a blank line.

MessageGate supports the following MIME Content Types:

Multipart:

multipart/mixed; boundary="---=_NextPart_Nr."

Textbody:

text/plain; charset=ISO-8859-1

Binarybody:

application/octet-stream

For more details see Chapter 2.3.3 Message Content.

Content-Transfer-Encoding:

Encoding of MIME content. **mandatory**

7bit

8bit

quoted-printable

base64

binary

Content-Disposition:

File name of MIME content, optional.

2.3.2 Address format

This Chapter describes the address format of “To:”, “Cc:”, “Bcc:” and “From:” header elements. The address has two parts, an Alias and a RFC822 address part.

The Alias part is used to define the X.400 address. The RFC822 part is divided into domain “@viat.de” and a surname that may have the value “x” or “User-ID” (*BusinessMail X.400* internal identifier) of a partner.

Possible address forms are:

a) Addressing partner using X.400 address in Alias:

   "X.400 address elements, separated by semicolon" <x@viat.de>

   This address form should be used if there is no partner profile and no User-ID entry configured for this partner or if a transfer to a Delivery Unit (e.g. FAX Gateway) is required. When sending an X.400 message the "MessageGate" process will use the parameters configured in the user profile to determine the syntax of the message. When delivering messages MessageGate will use this address if it does not find a User-ID entry in the database for the originator of the message.

   Example: "c=de;a=viat;o=testteam;s=tester;g=first" <x@viat.de>

   This address form may also be used to send messages to partners that do not have direct X.400 access but who are reachable via *BusinessMail X.400* gateways. A good example would be a message that is to be sent via the SMS gateway. In this case certain parameters that are necessary to define the SMS message have to be written into DDA address elements (SMS number, request reports …). The value of these elements can be changed for every SMS transaction/destination.

   "DDA:SMS=+4917111111111;DDA:ADR=Nein;DDA:DN=Ja;DDA:TIME=1440;S=SMS;O=Telekom;A=viaT;C=DE" x@viat.de

   When using the character ";" within an address field it has to be duplicated otherwise MessageGate will interpret it as a separator between address elements.

b) Addressing the partner using User-ID in the RFC822 address (Alias is empty)

   "" <User-ID@viat.de>

   This address form should be used if the trading partner is a Customer of *BusinessMail X.400* MailBox service or if an User-ID is already configured for an external partner (MessageGate or EDI partnership → *see also Chapter 2.5 Transmission Set File Format*).

   Example: "" <69365@viat.de>

c) Addressing Partner using X.400 address in Alias and User-ID in the RFC822 address

   "X.400 address elements, separated by semicolon" <User-ID@viat.de>

   This address form is used by the "MessageGate" process when delivering messages whose originator User-ID is in the database:

   Example: "c=de;a=viat;o=testteam;s=tester;g=first" 99999@viat.de

   If you use this address form when sending a message MessageGate will only use the X.400 address in the alias and will not verify the User-ID.

The maximum length of these addresses is 256 characters (alias + RFC822 address part). If this insufficient to enter a unique X.400 address we recommend that you configure a partner profile in order to address this partner only using the User-ID.

The following X.400 address elements (capital and small letters may be used for the element type and for the value but the value is not case sensitive) are valid for Alias:

C=xx;	Country code (2 characters Printable String, e.g. de)
A=xxxxx;	Name of ADMD (16 characters Printable String, e.g. viaT)
P=xxxxx;	Name of PRMD (16 characters Printable String, e.g. MGI)
O=xxxxx;	Organization (64 characters Printable or Teletex String, e.g. Tele kom)
OU1=xxxx;	Organization unit 1 (32 characters Printable or Teletex String)
OU2=xxxx;	Organization unit 2 (32 characters Printable or Teletex String)
OU3=xxxx;	Organization unit 3 (32 characters Printable or Teletex String)
OU4=xxxx;	Organization unit 4 (32 characters Printable or Teletex String)
DDA:xxx=xxxx;	Domain Defined Attributes (Type, 8 characters = Value, 128 characters, both Printable or Teletex String, e.g. service=fax)
S=xxxxx;	Surname (40 characters Printable or Teletex String)
G=xxxxx;	Given name (16 characters Printable or Teletex String)
CN=xxxxx;	Common name (64 characters Printable or Teletex String)
N-ID=xxxxx;	Box Identifier (Unique Agent ID, 32 characters Numerical)
X121=xxxxx;	Network Identifier (15 characters Numerical)
T-ID=xxxx;	Terminal Identifier (24 characters Printable String)
I=xx;	Initials (5 characters Printable String)
Q=xxx;	Generation (qualifier) (3 characters Printable String)

Some of these elements will be not used when sending X.400 messages depending on the parameter “X.400 Content-Type” in the host profile. For example the common name will not be used for “To:” and “From:” if the value of “X.400 Content-Type” is “IPM84”.

See also information about X.400 addresses in Chapter 2.8 Communication and Trading Relation Profile and in Appendix A: X.400 Address elements.

2.3.3 Message Content

The message content has to be defined in the header of a message in the element “Content-Type:”. A message can be sent with one body part or several (multipart) body parts/documents.

When sending (upload to file interface) a message with only one binary body the value of the element “Content-Transfer-Encoding:“ has to be set to either Base64 (7 Bit encoding) or Binary (8 Bit encoding). The parameter in the host profile defines the content transfer encoding MessageGate will use when delivering a message to the file interface.

When sending several documents in one message the value of the first element “Content-Type” has to be “multipart/mixed“ with a definition of a boundary character string. This boundary character string then separates the subsequent body parts with the “Content-Type” definitions for the individual body parts.

When mapping the contents of a message into an X.400 message the MessageGate process will use two host profile parameters “X.400 Content-Type“ and “Bodypart“ to create this X.400 message.

The host profile parameter “X.400 Content-Type“ will determine the format of the X.400 message. The default for this parameter is “IPM88” and should be not changed in the user profile. Only in exceptional circumstances (e.g. problems when using CommonName in the address) should the value “IPM84” be used in partnership profiles.

The following rules will apply in mapping the content of an uploaded message into the corresponding X.400 body parts when the value of the communication profile parameter “Bodypart” is set to “variable”.

Text body:

text/plain; charset=ISO-8859-1

- Content-Transfer-Encoding:
  - 7 Bit
  - 8 Bit
  - quoted-printable
- Content-Disposition:
  - Attachment; Filename = < file name >

will be mapped to

- General Text body part, ISOLATIN1 (ISO 8859-1) character set, or IA5 IRV Repertoire if a message is sent to an external mail services that only supports the 1984 X.400 Standard. When downgrading to the 1984 Standard the characters above 7Fh will be not converted.
- A file name defined in the “Content-Disposition“ element will force the MessageGate process to create a BP15 FTBP (FTAM body part) and provide this file information to the recipient. If the partner does not support FTBP do not add a file name to the text content or create a relation for this partner using Bodypart Mapping “IA5-text” or “ISO-Latin-1”.

Binary body:

application/octet-string

- Content-Transfer-Encoding:
  - base64
  - binary

will be mapped to

- Body part 14

application/octet-string

- Content-Transfer-Encoding:
  - base64
  - binary
- Content-Disposition:
  - Attachment; Filename=<file name>

will be mapped to

- Body part 15 (FTAM body part, FTBP), if value in profile is IPM88;
- Body part 14 (Bilaterally defined body part), if value in profile is IPM84, the name will be not mapped.

Multipart body:

multipart/mixed; boundary="---=_NextPart_xxx….."

The individual body parts have to be defined using the rules described above.

Change the value in the parameter "Bodypart" in the partner profile if your partner can only process the same type of X.400 body part and your application cannot adapt to this. *See more details about this parameter in Chapter 2.8 Communication and Trading Relation Profile.*

See Appendix C: for several examples of messages with different content types.

The MessageGate process will use the following rules when delivering messages to the file interface:

Single Text body:

- General Text body part or IA5Text
- ISOLATIN1 character set or IA5 Repertoire

will be mapped to

- Content-Type:
  - text/plain
- Content-Transfer-Encoding:
  - 8 Bit

Single Binary body:

- Bodypart 14 (BP14)

will be mapped to

- Content-Type:
  - application/octet-string
- Content-Transfer-Encoding:
  - binary/base64 (depending on parameter value in host profile)

- Body part 15 (FTAM body part, FTBP)

will be mapped to

- Content-Type:
  - application/octet-string
- Content-Transfer-Encoding:
  - binary/base64 (depending on parameter value in host profile)
- Content-Disposition:
  - Attachment; Filename=<file name>

Multibodypart:

will be mapped to

multipart/mixed; boundary="---=_NextPart_xxx….""

The individual body parts have to be defined using the rules described above.

Please take note of the following potential issues when implementing applications:

- Older X.400 E-Mail clients may not support BP15/FTBP and will attach the body part/document file information in a separate IA5 text body (so called CDIF information) before attaching the data in a binary body part (BP14). MessageGate will use this file information when delivering messages to the file interface and will directly add the file name in the Content Disposition element preceding this binary body. So the number of body parts mapped to the delivered message will decrease.
- The X.400 standard only defines a small number of body part types whereas in the MIME standard a large number of applications have defined their own specific content types. MessageGate attempts to analyze the start of the body part based on preconfigured pattern recognition in order to set a correspondent MIME content type. At present only the patterns for EDIFACT and PDF are used in this so called *DOCMAGIC* function.

2.4 The Forwarding of a message is not supported

The MessageGate File Interface does not support the forwarding of a delivered message. If a partner forwards a message to a MessageGate File Interface user only the user data (pay load) will be provided in the message file. There will be no information about the forwarded message itself.

2.5 Transmission Set File Format

2.5.1 The central EDI function

When using the central EDI function (has to be ordered separately) of *BusinessMail X.400* it is not a requirement to use the SMTP syntax to address your partner. You can simply upload one or several EDIFACT interchanges in one Transmission Set file via the file interface and the central EDI function will process this file.

MessageGate will use the information stored in EDI partnership entries in the database to add the X.400 address of the partner. At the present time the central EDI function only supports the sending or the receipt of one EDIFACT interchange per X.400 message in either a text body or a binary body part (BP14). The central EDI function at the present time will deliver only Transmission Set files that include one EDIFACT interchange to the MessageGate file interface.This restriction might be removed in one of the next versions of MessageGate, so any prospective applications should be designed to be able to handle received Transmission Set files that include more than one EDIFACT interchange.

When the central EDI function is activated all messages sent by partners, that include more than one EDIFACT interchange or one EDIFACT interchange and other documents will be rejected with a Non Delivery Notification ("Invalid arguments"→ Reason:1, Diagnositic:11) to the partner's X.400 address. When checking the status of such delivered messages entries for such rejected messages will be found.

The EDIFACT interchange included in the Transmission Set file will be attached to X.400 message based on the MessageGate parameter "bodypart" configured in the host based EDI trading relation profile. The default is text body (ISO-Latin1). If the trading partner requests the document as a binary body part the parameter has to be change to "Bilateral Bodypart 14". The Content Type "EDI" should be used only if your partner does not support another message type. In this case the same restriction of one EDIFACT interchange per received X.400 message applies, otherwise the PEDI (X435) message will be refused.

When using the central EDI function a MessageGate user has to have at least one EDI account. This EDI account consists of an EDI ID/ Reference Number (e.g. ILN or GLN) and an optional EDI Qualifier (e.g. "14" for commerce or "65" for X.400). MessageGate will either check or use this ID in the UNB EDIFACT header:

- the EDI sender when sending an X.400 message
- the EDI receiver when delivering an X.400 message

By default the central EDI function will deliver an EDIFACT interchange to a MessageGate user if the EDI-ID in the UNB matches the EDI-ID configured in the EDI account. In addition it is possible to setup a Closed User Group (CUG) for each individual EDI account. If this CUG is activated, only an EDIFACT document sent by a preconfigured EDI Trading partner will be delivered to the file interface.

An EDI Trading Relation entry has to be configured for each partner that a MessageGate user wants to address via the central EDI function (ie. send messages to). This entry includes the partner's EDI identifier and his X.400 address as well as a test-flag entry. The test flag in the UNB header of an interchange can be used by a partner as routing information if he wants differentiate between his live and his test environment (address) using the same EDI identifier. It is also possible to assign an EDI Trading

Relation to one or several of a MessageGate user's EDI accounts. The parameters in a EDI Trading Relation will define how to create an X.400 message.

Dependent of the settings of the host profile parameter "Map requested Report into" MessageGate will use the following notification settings in an X.400 message:

0 → Requests Non Delivery Notification (NDN)

1 → Requests Delivery Notification (DN)

2 → Requests Receipt Notification and Delivery Notification (RN and DN)

For more information please also see Chapter 2.8.2 X.400 Reports.

Please be aware that when using the central EDI Function the "MessageGate" process will not check the content of an EDI interchange, but it will check the syntax of the UNA, UNB and UNZ segments. If a syntax error is identified (e.g. no space in UNA or reference number in UNB and UNZ is different) the document will not be processed. In such a case MessageGate will send a 'Non Delivery Notification' with Diagnostic Code '0B'H (11 decimal, Invalid Arguments) when receiving this message. If MessageGate identifies a syntax error but is not able to identify an EDIFACT content, it will deliver the message to the file interface. For uploaded interchanges if MessageGate identifies a syntax error it will set the status to error. If the X.400 originator of a message uses a wrong ILN or if there is no EDI Trading Relation (Closed User Group) MessageGate will send a 'Non Delivery Notification' with Diagnostic Code '11'H (17 decimal, No bilateral Agreement).

In order to receive information over messages that have been refused a status report can be submitted via the file interface. Use the value "Both" or "Received" for the element "Direction:" to list entries of received (and also refused) messages. For more information please also see Chapter 2.6 The Status Report.

2.5.2 The Content of Transmission Set Files

It is possible to upload two and more EDIFACT interchanges in one Transmission Set file. The interchanges can be separated by adding an empty line with <CR/LF> but this is not necessary.

The number of interchanges in one Transmission Set file is theoretically unlimited but it is recommended not to exceed a 100 interchanges. The size of a Transmission Set file may not exceed 100 MB.

MessageGate at the present time delivers a Transmission Set file to the MessageGate file interface that only includes one EDIFACT interchange. A future version of MessageGate may support two and more EDIFACT interchanges per message. Anyone developing an application should take this into account.

A parameter in the host profile defines whether MessageGate delivers an EDIFACT interchange in the form of a Transmission Set file or in the form of a message with MIME syntax to the file interface. For more information please also see Chapter 2.8 Communication and Trading Relation Profile.

2.6 The Status Report

2.6.1 General

MessageGate does not deliver X.400 reports to the file interface (only Messages/ Data). However it is possible to request a status report that provides information about the status of all messages processed by MessageGate (sent and delivered). The information for each transaction is stored in a database relation (Trace_Tab) for a predefined period of time. The Default Purge Time is 240 hours (ie. an entry will be deleted if it is older than 240 hours), but this value can be changed individually for each customer. When uploading a 'status report request' the MessageGate user receives information about the status of his messages in a structured file which can be imported into an application or a tracking tool.

When sending a message to several recipients an entry will be made in the status report for each recipient. In such a case the Message-ID and Order ID are only unambiguous in combination with the recipient address while processing the entry.

Be aware that the logical sequence of these entries may be different to the sequence of recipients in the MIME header.

There will only be one entry for a delivered message, also if the originator sent the message to several recipients. The recipient list is displayed in the MIME header of the delivered message file.

The address displayed in the status report is identical to the address in the MIME header of the message and also the type of address will be unchanged. The type of address is displayed always in the same manner (first character: capital letter, subsequent characters: small letter) → "To:", "Cc:" and "Bcc:".

2.6.2 Request a Status Report

MessageGate provides status reports on request (S_Order-ID.IN) or automatically if configured in the host profile (configuration via *WebConfig*, see Chapter 2.8.8 Configure automatically generated Status Report). *WebConfig* allows you to view status reports or to download those reports in structured files (CSV file), for more details please see Chapter 2.8.7 Request Status Report in WebConfig.

To reduce the amount of information (number of entries) included in status reports MessageGate provides different selection criteria. One can select only one entry (using Order ID or Message-ID) and request to receive the whole message history (readable or CSV format) instead of only the present message status.

MessageGate offers the following selection criteria/parameter in a 'status report request':

- whether the status of an entry has changed since the last status report or not
- whether a message was sent or delivered
- only defined Message-ID or part of it
- only defined Order ID or part of it
- date/time when a message was sent or delivered

An additional parameter defines whether to indicate the actual message status or the whole message status history.

Parameter: Value	**Explanation:**
Disposition: All	Select all messages, independent of whether the status has changed or not (Default).
Disposition: Modified	Select all messages where the status has changed since the last status report (e.g. received DN or RN).
Direction: Sent	Only select sent messages (Default).
Direction: Received	Only select received messages.
Direction: Both	Select sent and received messages.
Format: Actual	Show only the present status of messages and the timestamp of the last status change (Default).
Format: History	Show all changes of status and their respective timestamp (Sent/ received message, Received DN/NDN, sent/ received RN/NRN).
Format: CSV-S	Show all changes of status and their respective timestamp (Sent/ received message, Received DN/NDN, Sent/ received RN/NRN) using CSV semicolon separated format.
Format: CSV-C	Show all changes of status and their respective timestamp (Sent/ received message, Received DN/NDN, Sent/ received RN/NRN) using CSV colon separated format.
Message-ID: xxx*	Only show those messages where Message-ID starts with a predefined string. Always use "*" for a wildcard or partial wildcard search.
Order-ID: xxx*	Only show those messages where Order ID starts with predefined string. Always use "*" for a wildcard or partial wildcard search. The Order-ID is case sensitive.
Since: dd-mmm-yyyy hh:mm:ss	Select only those entries stored in the Trace_Tab after the defined date/time. When only a date is defined, all entries from this date (starting at 00:00) will be selected.

There are default values for the first two criteria/parameters and also for the format that MessageGate will use if there is no definition in a 'status report request'. The number of returned entries can be limited further using additional criteria in the 'status report request' (logical "AND"- combination).

If MessageGate will use the three default values, all sent message entries stored in the database (Trace_Tab, not deleted by the "Purger" process) will be written to the status report file, independent of whether the status has changed since the last 'status report request' or not. Each entry will only display the status of the last message transaction but not its history.

2.6.3 Status Report Syntax (readable structure)

If MessageGate has processed a 'status report request' (S_Order-ID.IN) it will select those entries based on the selection criteria and create a status report file. For this report file the same filename as the 'status report request' file is used, but with the ".OUT" file extension.

Please ensure that your application only uses a unique Order-ID in the name of the 'status report request' file. The operating system on which the MessageGate application is hosted on will not replace the existing 'status report request' files. Instead it will store the new file using a higher version number. WebDAV clients will not exhibit these version numbers. These version numbers may cause problems in your application.

The content of the status report file consists of header information and message entries. The first line in this header information shows the User-ID of the MessageGate User and a timestamp for this report. The second line displays the filter criteria used to create this report.

Separated by an empty line (CR/LF) the message entries follow this header information.

Depending on the selected criteria "Format" a message entry may consist of 6 (Format:actual) or 5-7 lines (Format:history). The information regarding sender/recipient, Order-ID, Message-ID and MTS/MTA ID are available in both formats. Only the status information differs between both formats.

Syntax of the first line of the header information

Status Report for UserID xxxxx; generated dd-mmm-yyyy hh:mm:ss

The UserID value field has a minimum of 4 digits, but values of up to 6 digits are also possible.

The timestamp element "dd" defines the day of month (no leading zeros in case of one digit values), "mmm" the name of month (English abbreviation), "yyyy" the year, "hh" the hours (24 hour schema, with a leading zero in case of one digit values), "mm" the minutes (with a leading zero in case of one digit values) and "ss" the seconds (with a leading zero in case of one digit values). The timestamp is always in MET or MEST, (see also the syntax of the message entry).

Example:

Status Report for UserID 4911; generated 13-Sep-2010 13:43:32

Status Report for UserID 23423; generated 7-Sep-2010 07:12:01

Syntax of the second line of the header information

Filters: Disposition=x, Direction=x, Format=x, Message-ID=x, OrderID=x, Since=dd-mmm-yyyy

There are no spaces between the filter criteria and the corresponding value. The individual filter parameter are separated by the "," (comma) and " " (space) character. MessageGate always adds the "Disposition=", "Direction=" and "Format=" criteria fields. The others criteria fields are only displayed if they have been defined in the 'status report request'.

The possible values of the selection criteria fields:

- "Disposition=" ["All" | "Modified"]
- "Direction=" ["Sent" | "Received" | "Both"]
- "Format=" ["Actual" | "History"]

- "Message-ID=" the selection criteria value used or the selection criteria will be not displayed.
- "Order-ID=" the selection criteria value used or the selection criteria will be not displayed
- "Since=" date in the form (dd-mmm-yyyy hh:mm:ss).used or the selection criteria will be not displayed. Please consider the "lifetime" of entries in the database (so called 'Purge Time' used in the Trace_Tab).

Example:

Filters: Disposition=All, Direction=Both, Format=Actual, Since=1-Jan-2009

➔ All entries for sent/received messages since 01.01.2009 00:00:00 and which are still stored in the database are selected independent of whether the status has changed will be displayed with their actual status.

Filters: Disposition= Modified, Direction=Received, Format=History

➔ All entries for received messages where the status has changed since the last report will be displayed with detailed status information.

Filters: Disposition= Modified, Direction=Sent, Format=History, Order-ID=EDI*

➔ All entries of sent messages where the status has changed since the last report and where Order ID starts with "EDI" will be displayed with detailed status information.

Syntax of sent message entries with "Format"="Actual"

Each line consists of a field type followed by a semicolon ":", a space " " and the field value that may also include spaces. The type of recipient address can be "To:", "Cc:" or "Bcc:".

To:	Recipient address (when using the central EDI function the address is always of the form"" <user-id@viat.de>)
Cc:	Carbon copy recipient address
Bcc:	Blind carbon copy recipient address
Order-ID:	Order number also defined in the file name (maximum 22 characters)
Message-ID:	Message number defined in the SMTP Message or when using central EDI function the Interchange Control Reference ID of the EDIFACT interchange (maximum 64 characters)
MTS-ID:	The MTS identification used by the MTA when the message was sent (maximum 32 characters)
Status:	The actual message status (for possible values see below)
Date:	Timestamp of last status change in the format dd-mmm-yyyy hh:mm:ss +xxxx, where "dd" is day of month (no leading zero in case of one digit value), "mmm" is the month name (English abbreviation), "yyyy" is the year, "hh" is the hour (24 hour, with leading zero in case of one digit value), "mm" is the minute (with leading zero in case of one digit value) and "ss" is seconds (with leading zero in case of one digit value). The value +xxxx shows the time difference to UTC/GMZ, so +0100 for MET or +0200 for MEST (daylight saving time).

Syntax of received message entries with "Format"="Actual"

Each line consists of a field type followed by semicolon ":", a space and the value that may also include spaces.

From: Originator address

Order-ID: Order number assigned by MessageGate (maximum 22 characters)

Message-ID: Message identification assigned by the message originator (maximum 64 characters)

MTS-ID: Message identification assigned by originating MTA (maximum 32 characters). This will be mapped to the element X-MPDUID in the SMTP header.

Status: The actual message status (for possible values see below)

Date: Timestamp of last status change in the format dd-mmm-yyyy hh:mm:ss +xxxx, where "dd" is day of month (no leading zero in case of one digit value), "mmm" is the month name (English abbreviation), "yyyy" is the year, "hh" is the hour (24 hour, with leading zero in case of one digit value), "mm" is the minute (with leading zero in case of one digit value) and "ss" is seconds (with leading zero in case of one digit value). The value +xxxx shows the time difference to UTC/GMZ, so +0100 for MET or +0200 for MEST (daylight saving time).

Syntax of sent message entries with "Format"="History"

Each line consists of a field type followed by colon ":", a space " " and the field value that may also include spaces. Please be aware that the number of status entries is variable and that the entries are interdependent (i.e. for a "READ" status it is necessary that there are entries for a "Sent" and "Delivered" status). A negative Report/ value will terminate the transaction so that there can be no more status entries for this message. The type of recipient address can be "To:", "Cc:" or "Bcc:".

To: Recipient address (when using the central EDI function the address is always of the form "" <user-id@viat.de>)

Cc: Carbon copy recipient address

Bcc: Blind carbon copy recipient address

Order-ID: Order number also defined in the file name (maximum 22 characters)

Message-ID: Message number defined in SMTP Message or when using the central EDI function the Interchange Control Reference ID of the EDIFACT interchange (maximum 64 characters)

MTS-ID: The MTS identification used by the MTA when the message was sent (maximum 32 characters).

Sent: Time stamp of sent message
Format:
dd-mmm-yyyy hh:mm:ss +xxxx, where "dd" is day of month (no leading zero in case of one digit value), "mmm" is the month name (English abbreviation), "yyyy" is the year, "hh" is the hour (24 hour, with leading zero in case of one digit value), "mm" is the minute (with leading zero in case of one digit value) and "ss" is seconds (with leading zero in case of one digit value). The value +xxxx shows the time difference to UTC/GMZ, so +0100 for MET or +0200 for MEST (daylight saving time).

Or

Error: When MessageGate fails to process a message file or fails to send a message/document error information will be created and will displayed with a respective timestamp in this entry
Format:
Error: dd-mmm-yyyy hh:mm:ss (Reason: nnnnnnnn, Diagnostic: n)

Delivered: Timestamp of when the message was delivered into recipient's mailbox (Format: see Sent:)

Or

Failed: Message was not delivered and the MTA created a Non Delivery Notification (NDN) that includes information about the problem
Format:
Failed: dd-mmm-yyyy hh:mm:ss (Reason: n, Diagnostic: n)

Read: Time stamp when recipient has processed/ read message (Format see Sent:)

Or

Denied: Message was deleted or discarded by recipient
Format:
Denied: dd-mmm-yyyy hh:mm:ss (Reason: n, Diagnostic: n)

Syntax of received message entry with "Format"="History"

Each line consists of a field type followed by a colon ":", a space " " and the field value that may also include spaces. Please be aware that the number of status entries is variable and that the entries are interdependent (e.g. for "READ" it is necessary that there is an entry for a "Received" status). Negative Reports/ values will terminate the transaction so that there will be no more status entries for this message.

From: Originator Address

Order-ID: Order-ID set by MessageGate (maximum 22 characters)

Message-ID: Message-ID the originator sets in the message (maximum 64 characters)

MTS-ID: The MTS identification defined by the sending MTA (maximum 32 characters). The element X-MPDUID in the SMTP header will show same value.

Received: Time stamp Received message
Format:
dd-mmm-yyyy hh:mm:ss +xxxx, where "dd" is day of month (no leading zero in case of one digit value), "mmm" is the month name (English abbreviation), "yyyy" is the year, "hh" is the hour (24 hour, with leading zero in case of one digit value), "mm" is the minute (with leading zero in case of one digit value) and "ss" is seconds (with leading zero in case of one digit value). The value +xxxx shows the time difference to UTC/GMZ, so +0100 for MET or +0200 for MEST (daylight saving time).

Or

Failed: Message was not delivered

Format:
Failed: dd-mmm-yyyy hh:mm:ss (Reason: n, Diagnostic: n)

Read: Time stamp for Sent Receipt Notification
Format:
Read: dd-mmm-yyyy hh:mm:ss +xxxx, where “dd” is day of month (no leading zero in case of one digit value), “mmm” is the month name (English abbreviation), “yyyy” is the year, “hh” is the hour (24 hour, with leading zero in case of one digit value), “mm” is the minute (with leading zero in case of one digit value) and “ss” is seconds (with leading zero in case of one digit value). The value +xxxx shows the time difference to UTC/GMZ, so +0100 for MET or +0200 for MEST (daylight saving time).

Or

Denied: Information for sender that message was discarded
Format:
Denied: dd-mmm-yyyy hh:mm:ss (Reason: n, Diagnostic: n)

Status of sent messages:

Sent

Error: (Reason: nnnnnnnn, Diagnostic: n)

Delivered

Failed: (Reason: n, Diagnostic: n)

Read

Denied: (Reason: n, Diagnostic: n)

Status of received messages:

Received

Failed: (Reason: n, Diagnostic: n)

Read

Denied: (Reason: n, Diagnostic: n)

See also Appendix C for more examples.

2.6.4 Syntax of Status reports (CSV structure)

If MessageGate has processed a ‘Status report request’ (S_Order-ID.IN) it will select those entries defined in the selection criteria and create a report file. It will use the same file name but with the “.OUT” extension. Please be aware that the CSV format is optimized for automatic processing and so it is difficult to read.

The content of the status report file consists of header information and message entries. The header information in the first line contains the User-ID of the MessageGate User and a timestamp for this report. In the second line the filter criteria used for this report are displayed.

Unlike the report format described in the last Chapter the header of the CSV format contains additional information. Separated by an empty line (CR/LF) there is another line containing the field identifier, the field name.

Field name:	**Explanation:**
From	In the received message the originator address (Alias/X.400 address + RFC822 address, maximum 256 characters). Quotation marks will be used for the alias and also within the CSV structure for string declaration, so this field will start with three quotation marks, two quotation marks will follow the alias address and at the end of the field another quotation mark will define the end of this string. (""""G=test;S=tester1;O=testag;A=viaT; C=de"" 95344@viaT.de").
To	The recipient address used in the submitted message (Alias/X.400 address + RFC822 address, maximum 256 characters). Format see “From:“. Address type see Rcpt Type.
Order-ID	Order identifier defined in the file name (maximum 22 characters) within quotation marks.
Message-ID	Message identifier or reference number of EDIFACT interchanges within transmission set (maximum 64 characters) within quotation marks.
MTS-ID	Identifier generated by the MTA when sending a message (maximum 32 characters) within quotation marks.
Received	Timestamp (UTC/GMT) of receiving message (dd.mm.yyyy hh:mm) without quotation marks or “Failed“ if message could not be delivered (Error code see Reason und Diagnostic).
Sent	Timestamp (UTC/GMT) of sent message (dd.mm.yyyy hh:mm) without quotation marks or “Error“ if message could not be sent (Error code see Reason und Diagnostic).
Delivered	Timestamp (UTC/GMT) of delivery time of a

	sent message (dd.mm.yyyy hh:mm) without quotation marks or “Failed“ if message could not be delivered (Error code see Reason und Diagnostic).
Read	Timestamp (UTC/GMT) when a sent message was processed (dd.mm.yyyy hh:mm) without quotation marks or “Denied“ if message had been discarded (Error code see Reason und Diagnostic).
Reason	Reason code for a failed action (for details see Appendix B) without quotation marks.
Diagnostic	Diagnostic code for a failed action (for details see Appendix B) without quotation marks.
Errordate	Timestamp (UTC/GMT) for a failed action (dd.mm.yyyy hh:mm) without quotation marks.
Rcpt Type	Recipient address type : To, Cc or Bcc.

2.7 Send Receipt Notification

It is possible to send a positive or negative Receipt Notification (RN) for each delivered message if the originator has requested this in his message. MessageGate will display this request in the header element “Disposition-Notification-To: <X.400 Originator Address>“ of delivered SMTP message.

It is also possible to configure in the host profile that a requested RN will be not mapped into an SMTP message so that the structure of the header does not change.

To send a Receipt Notification create a file where file name includes the Order-ID of delivered message.

The format of file name is: „R_<Order-ID of delivered message>.IN“.

MessageGate will use the following values defined in file to create the X.400 reports:

Processed→ Receipt Report/Notification (RN)

Failed → Non Receipt Report/Notification (NRN) with Reason Code “0” (Discarded)

Other values in the file will cause MessageGate to refuse this request and to add an error code to the file name.

Please be aware that the sending of Receipt-Notifications is a chargeable item!

2.8 Communication and Trading Relation Profile

2.8.1 General

It is necessary to configure a communication profile for each user of the MessageGate file interface. This profile defines the rules of how to map the content of a SMTP message into an X.400 message and how to build the header of the X.400 message.

With an existing communication profile a MessageGate user is able to send to and receive messages from X.400 partners and is also able to use the *BusinessMail X.400* Gateway services (Fax-Gateway, SMS-Gateway and the Internet/SMTP-Gateway). For these cases MessageGate will use the definitions stored in the communication profile to create X.400 messages.

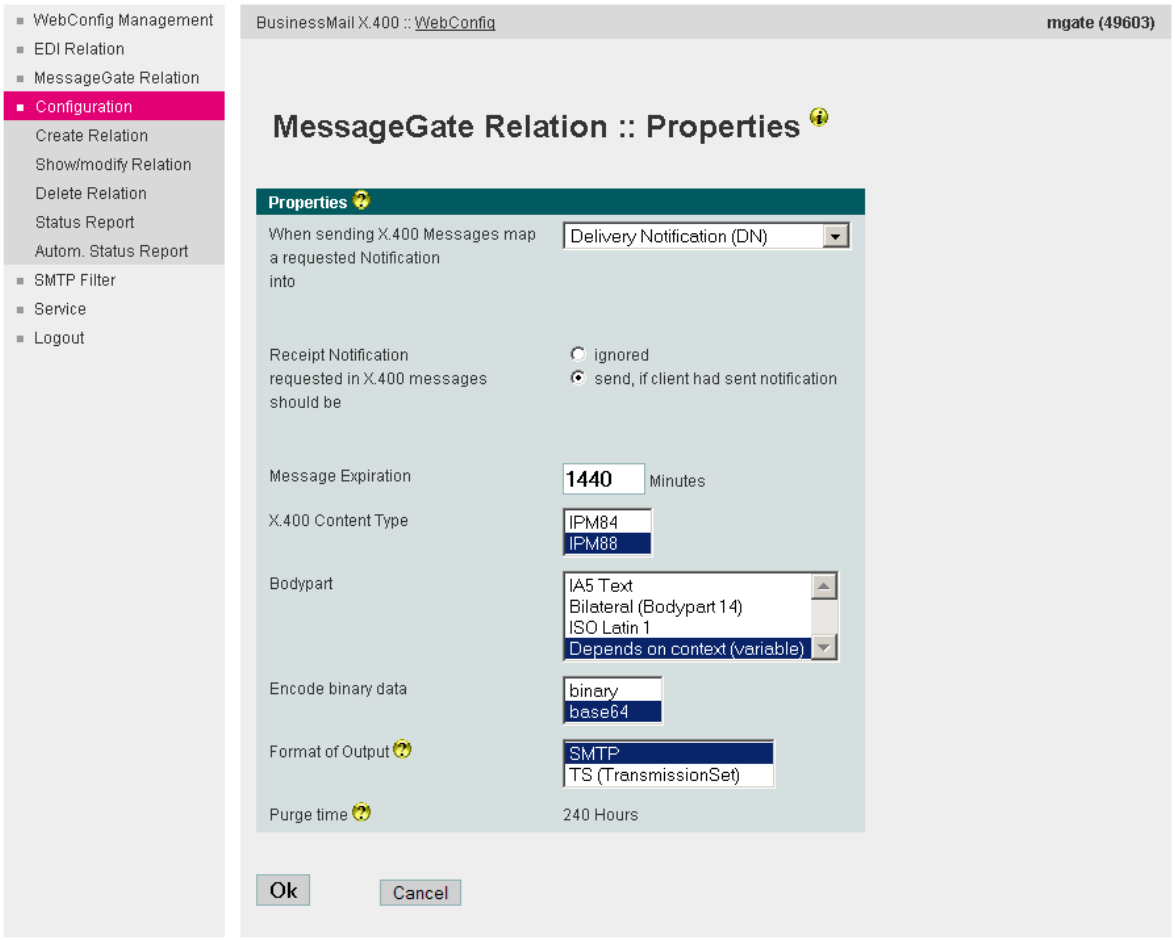
The configuration of separate Trading Relation Profiles is only necessary if the trading partner requires a special message type/content or if non-default Notifications is required for this Trading Relation. The *BusinessMail X.400* central Administration will configure a Trading Relation Profile on request but this service is chargeable. Hence we recommend the use of *WebConfig*, a *BusinessMail X.400* Web-based application which allows, amongst other services, the administration of Trading Relations.

All standard Web browsers (enable Java-script to facilitate the use of all the offered functions) are supported for the access to the *WebConfig* application (URL https://WebConfig.viat.de/WebConfiglogin). In order to use *WebConfig* one has to first download a Client certificate (check the *BusinessMail X.400* Service URL: http://www.service-viat.de) and to import this certificate into the selected Web browser before trying to access the *WebConfig* application. At this stage the use of cookies has to be enabled. When accessing the *WebConfig* application the *BusinessMail X.400* proxy Server will request this certificate for each connection. The *WebConfig* application itself will prompt for Username and Password in order to authenticate the *WebConfig* user. This Login data is configured when your MessageGate account is provisioned. If you do not receive this information please contact the *BusinessMail X.400* Helpdesk. After the login into your *WebConfig* account you may download a personified certificate and modify the properties of your *WebConfig* account so that this certificate will be used to authorize the access to your *WebConfig* account.

The main *WebConfig* menu contains the following menu items dependent on the subscribed features:

- User administration to change the *WebConfig* password; verify the change log; download data (certificates, EVN, parameter files); modify the properties of the *WebConfig* Account (time zone and separator for CSV files, GUI language selection and cookie lifetime).
- Administration of MessageGate Trading Relations
- Administration of EDI Trading Relations
- Administration of SMTP/Internet Trading Relations (SMTP Filter)
- Access to extended service information

The following screen shot shows the menu items of a MessageGate user where the central EDI function is activated.



Under the menu item “MessageGate Relation - Properties“ the default communication parameters for all partners are displayed and in the “MessageGate Relation - Create, Show/Modify or Delete“ menu items the communication parameters for special Relations can be configured. The values configured in menu item “MessageGate Relation - Properties“ will be used as the initial values when starting to configure new Relations. *WebConfig* will ask you whether you also want to modify the existing relations or not when changing some of these parameters.

2.8.2 X.400 Reports

The X.400 standard offers different report types (Delivery- or Receipt-Notifications) to verify the status of a message / a transaction. By default MessageGate will request a Delivery-Notification in an X.400 message when “Disposition-Notification-To” is defined in the SMTP message. However this can be modified in the communication profile or in a Trading Relation profile:

- Non-Delivery-Notification → Send a Report only if the message cannot be delivered to the recipient
- Delivery Notification → Send Report if the message was delivered to the recipient’s mailbox (also implies Non-Delivery-Notification)
- Receipt-Notification → Send a Receipt Notification Message if the message was processed by the recipient (read/fetched). In this case a Delivery Notifica-

tion will also be requested and the receipt of a DN will be displayed in the status report.

If “Disposition-Notification-To” is not defined in the SMTP message an X.400 report will be not be requested. The MessageGate user will not receive any information if the delivery of a message has failed.

When sending documents via the central EDI function an X.400 report will always be requested based on the parameters configured in the host profile.

It depends on the acknowledgement mechanisms agreed between trading partners and the transferred data whether it is necessary to request X.400 reports or not. If there is already an acknowledgement mechanism defined at the application layer it may not be necessary to monitor the transport (X.400) layer and to request X.400 reports. However we recommend monitoring the delivery of a message into the partner’s mailbox. Please be aware when requesting a Receipt-Notification that the partner has to agree to send this type of report because the X.400 standard gives the recipient of a message the choice of sending or not sending a Receipt-Notification. The mapping of a Receipt-Notification to a sent message is only possible if the entry of this transaction in the Trace_Tab has not already been deleted by the “Purger” process.

Please be aware that the sending of Receipt-Notifications is a chargeable item within the context of the *BusinessMail X.400* service as well as with other X.400 service providers.

Select in the menu item “When sending X.400 Messages map requested Notification into“ the appropriate report mechanism (Default is Delivery Notification DN) for your environment.

The menu item “Receipt Notifications requested in X.400 Messages should be“ defines whether a request for Receipt-Notification in X.400 message should be mapped into “Disposition-Notification-To:“ of a delivered SMTP message or not. By default the request will be mapped but this setting may cause problems in certain applications so it is possible to suppress this in the host profile.

2.8.3 X.400 Header Information

The menu item “Message Expiration“ defines the expiration time of the X.400 message. The default value for the item “Message Expiration” is 1440 minutes (= 24 hours). This means the MTA or set of MTAs will try to deliver the message to a correctly addressed recipient for 24 hours before a Non Delivery Notification (NDN, if requested!) is created and sent back to the originator of the message.

The menu item “X.400 Content Type“ specifies the structure of the X.400 message. The item “X.400 Content Type“ defines the type of X.400 message that will be sent to a partner. Possible values are “IPM84” and “IPM88” (Default).

When using “IPM84” MessageGate will create an X.400 message of type P2 (X.400 Standard 1984) and it will support IA5 text body part and the binary body part (Bilaterally defined body part BP14 → Binary data without file information). In this case it will also not add the “Common Name” address element to the originator’s and recipient’s address. Use the value “IPM84” only if your partner has problems processing messages that MessageGate has sent to his mailbox (for example the partner is a Customer of a mail system that only supports the 1984 X.400 Standard or has problems processing the X.400 “Common Name” address attribute).

When using “IPM88” (default value for this item) MessageGate will create an X.400 message of type P22 (X.400 Standard 1988/92) and will also support BP15 FTAM body part (FTBP), that includes the binary data and additional file information (e.g. file name). MessageGate will also add the X.400 “Common name” address attribute to the originator’s and to the recipient’s address in the X.400 message.

If you are using the central EDI functionality to send messages the message type will be defined in the EDI Trading Relation. The central EDI functionality offers in addition the message type PEDI (X.435) to send the data (EDIFACT document).

2.8.4 X.400 Body parts

The item “Bodypart“ defines the mapping of MIME content into X.400 body parts when sending an X.400 message. It is possible to use the same body part type mapping (values: IA5-Text, Bilateral body part 14, ISO-Latin-1) or to map the MIME Content into equivalent X.400 body part (value: Variable). Variable is the default value for this item and should only be changed in a Trading Relation if your partner always requests the same X.400 body part and your application is not able to provide the equivalent MIME content type in all cases or your application will send MIME text content including a file name that has to be sent as an X.400 text body part.

Be aware when sending an X.400 message to different recipients, the MessageGate process will ignore existing Trading Relations and will use the mapping rules configured in the properties entries instead.

When sending documents via the central EDI function the mapping of an EDIFACT document to an X.400 body part will be defined in the EDI Trading Relation.

2.8.5 Encoding of binary data

This item defines whether MessageGate should use MIME Content Encoding Binary or Base64 when mapping an X.400 binary body part (BP14 or BP15/FTBP) into an equivalent MIME Content Type. All E-Mail clients should be able to open BASE64 encoded messages. When sending a message MessageGate will accept both types of Content Encoding.

2.8.6 File format (Format of output)

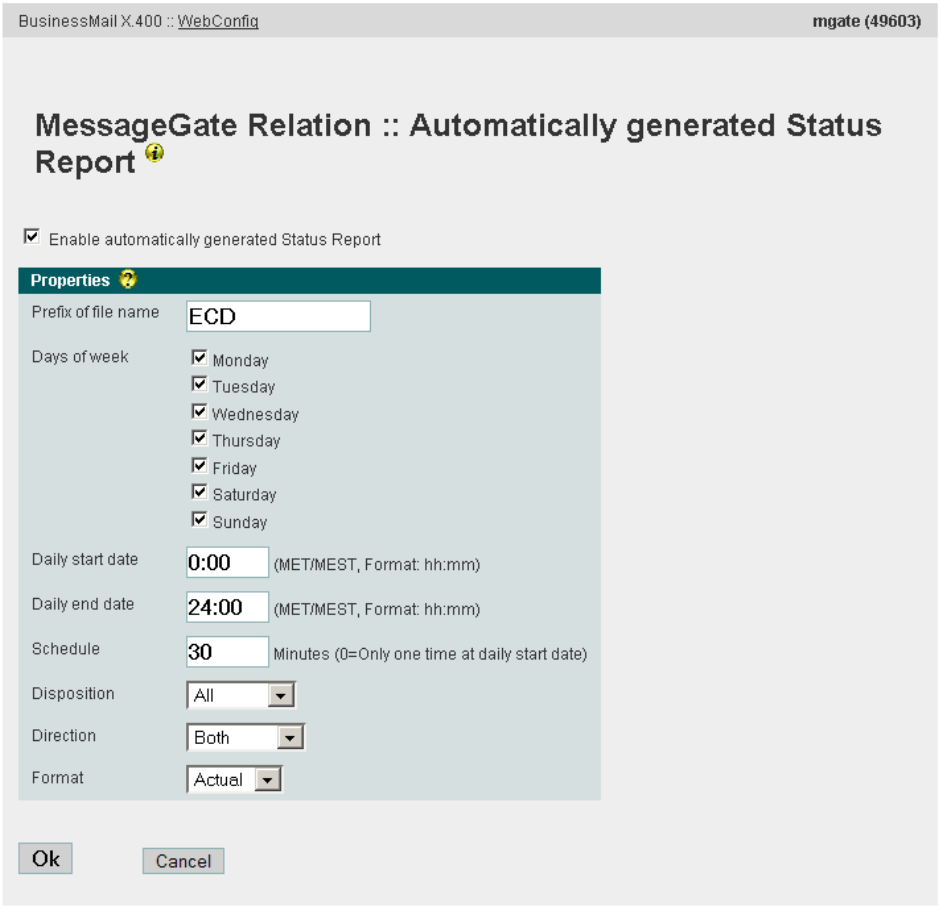
If the central EDI function is activated this item will define whether an EDIFACT document sent by a partner will be delivered in a SMTP structured file or in a Transmissions Set file. This menu item is only available in the base host profile and not in the Trading Relation profile.

2.8.7 Request Status Report in WebConfig

The menu item ”Status Report“ enables you to request the status of transactions (sent or received messages) and view it directly in the GUI or to download it in a CSV file or to open this file directly using an appropriate program (for example Microsoft Excel). You can restrict the number of displayed/stored entries by entering a date, by checking the box „Only failed messages“ or using a search string filter when selecting reports for viewing directly in the GUI. The character used as a separator in CSV file will be defined in properties of WebConfig Management. The default is semicolon.

2.8.8 Configure automatically generated Status Report

You can receive status reports in your MessageGate directory by requesting these via the MessageGate API or the periodic generation these status reports can be configured via *WebConfig*. This menu item defines the time when a status report should be generated (day of week, start time, end time) and the schedule (minimum is 30 minutes). A filename prefix can be defined for this file. MessageGate will add a timestamp to the file name to create a unique file name.

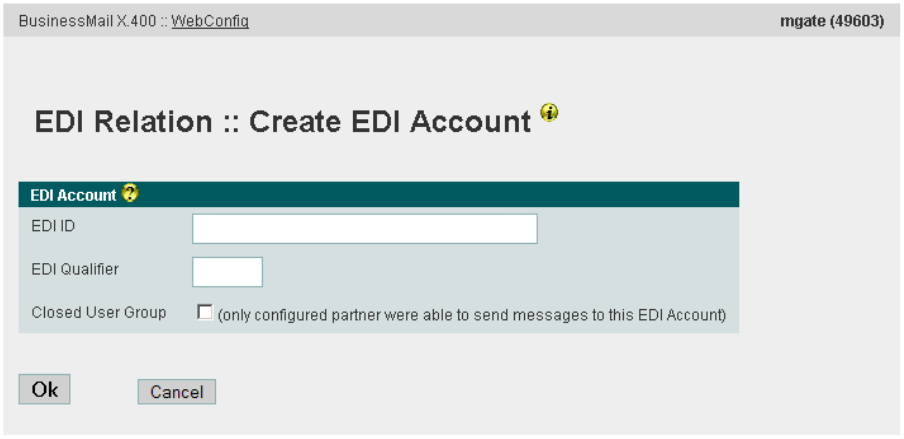


The content of these reports are defined by the selection criteria used (see also Chapter 2.6 The Status Report).

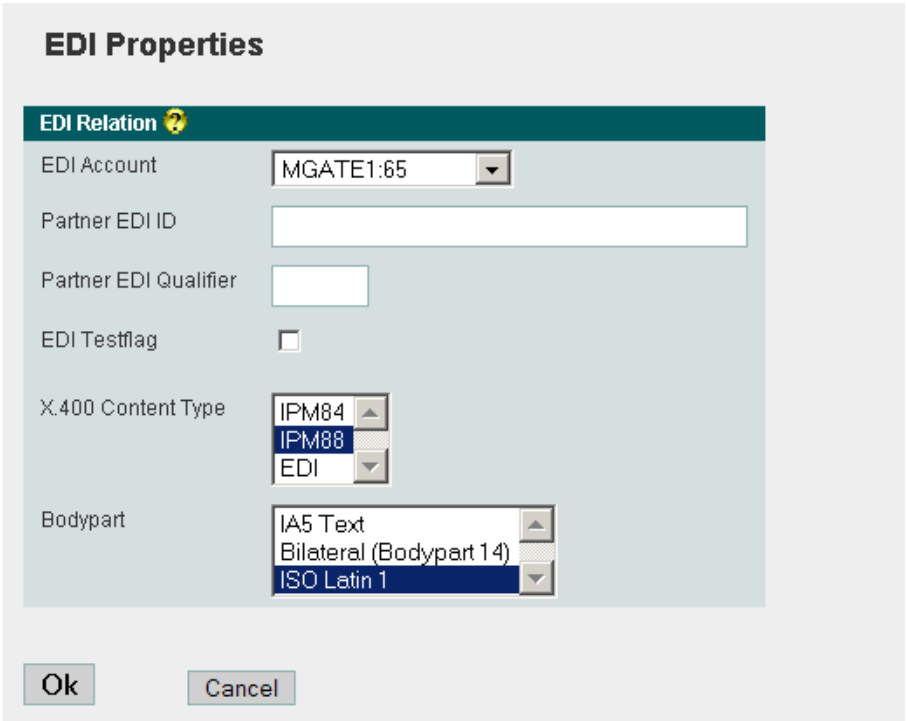
2.8.9 EDI Relation

If the central EDI functionality has been enabled for your MessageGate account a main menu item ”EDI Relation“ where you can configure your EDI accounts and your

EDI Relations should be displayed. If you want to use the central EDI functionality you have to configure a minimum of one EDI account. As long as no Closed User Group (CUG) has been enabled for this account, all your trading partners can send EDIFACT documents (one document/ interchange per message) to this account.



If you plan to send EDI documents to your partners you have to configure an EDI Relation for each partner, In this EDI Relation you have to add the X.400 address or an User ID (Mailbox X.400 internal identifier) to a partner's EDIFACT address (EDI ID, for example ILN/GLN and optionally an EDI Qualifier).

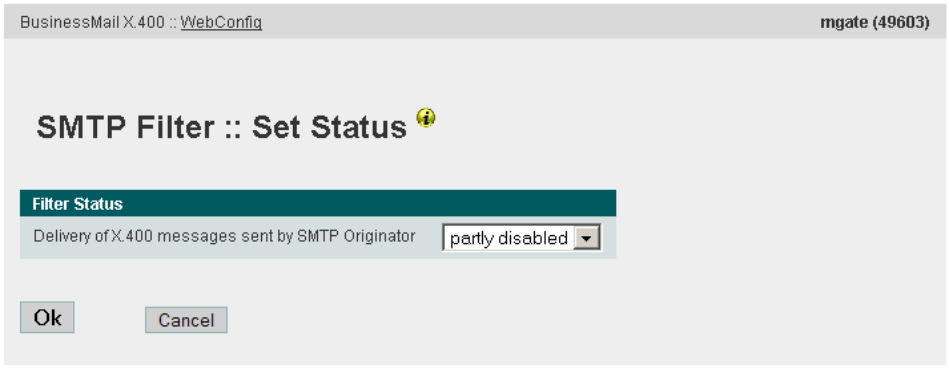


For an EDI Relation you may use the optional test flag in the UNB Header of an EDIFACT document to differentiate between the live and the test system of your partner. In this menu section you can define the format of an X.400 message and the type of body part sent to your partner.

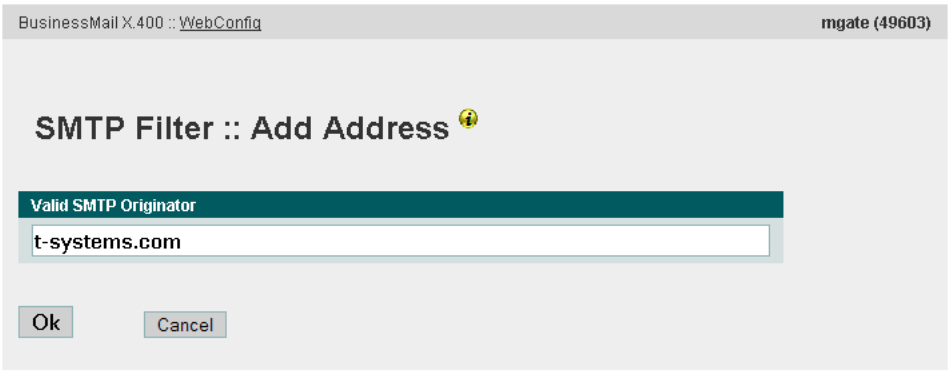
2.8.10 SMTP Filter

By default there are no restrictions in regard to Internet E-Mail users sending mails to your MessageGate account. However it is possible to setup a filter in the SMTP-

Gateway to prevent the delivery of mails sent by Internet E-Mail users or restrict it to configured partner/ domains.



Using the 'SMTP Filter:: Add Address' menu item complete E-Mail addresses or only parts thereof (for example the domain part) may be configured. If adding partial addresses no wild card characters should be used (see screenshot).

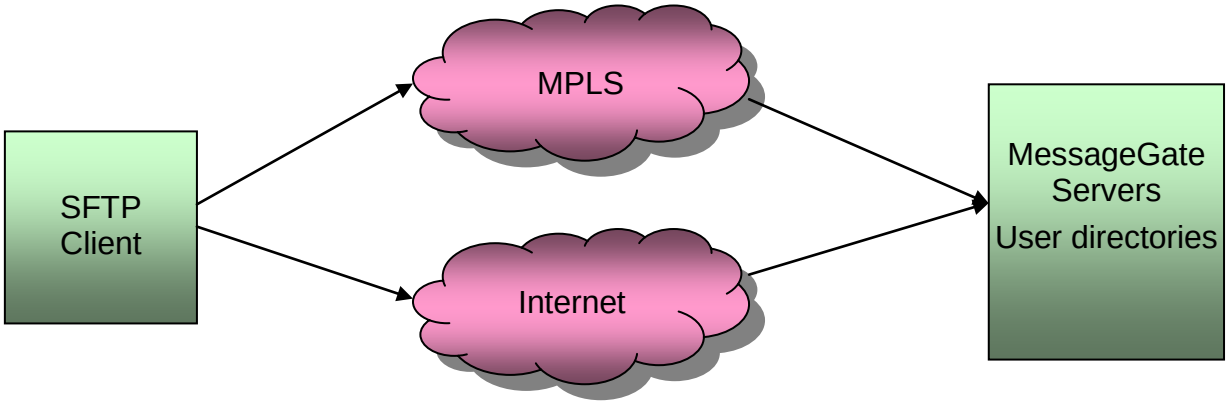


Please be aware that your configured address filter rules will only be effective if the 'SMTP Filter:: Set Status' menu item is set to 'partly disabled'.

3 Access via SFTP (SSH)

3.1 General

For network administrators the use of FTP may cause problems because FTP requires two TCP/IP sessions. As an alternative *BusinessMail X.400* offers the use SFTP (part of SSH suite using Port 22) for secure data transfer. Each MessageGate user will be configured on the Application server (OpenVMS) and the MessageGate directory will be the login directory. This means that it is possible to directly upload and download data from the Application server after a login into the SFTP account.



You can use MPLS or Internet to access *BusinessMail X.400* Application server.

To access your directory via Internet you may use the logical address “sftp.viat.de”.

3.2 Features to note

A client accessing *BusinessMail X.400* using SFTP will authenticate itself via a user name and the public key stored on the SFTP host and in turn the host will authenticate itself to the client with his own certificate. Different SFTP clients may use different types of public keys (to convert the different types we recommend the use of puTTYgen which is part of putty and the WinSCP product set). A potential SFTP user has to provide his public key (format SSH2) to the *BusinessMail X.400* administration who will store this key on the respective SFTP systems. A user may provide more than one public key. On the SFTP server systems each SFTP user has a user specific sub directory named SSH2 containing his public keys and a file named AUTHORIZATION. The file AUTHORIZATION defines all the valid keys. We recommend a key length of minimum 2048 bit when using SFTP communication. A SFTP user may copy new public keys directly into the SSH2 subdirectory, but only the *BusinessMail X.400* administration is able to modify the AUTHORIZATION file. Please ask the *BusinessMail X.400* Helpdesk to initiate this change.

3.3 Recommended SFTP Communication modules

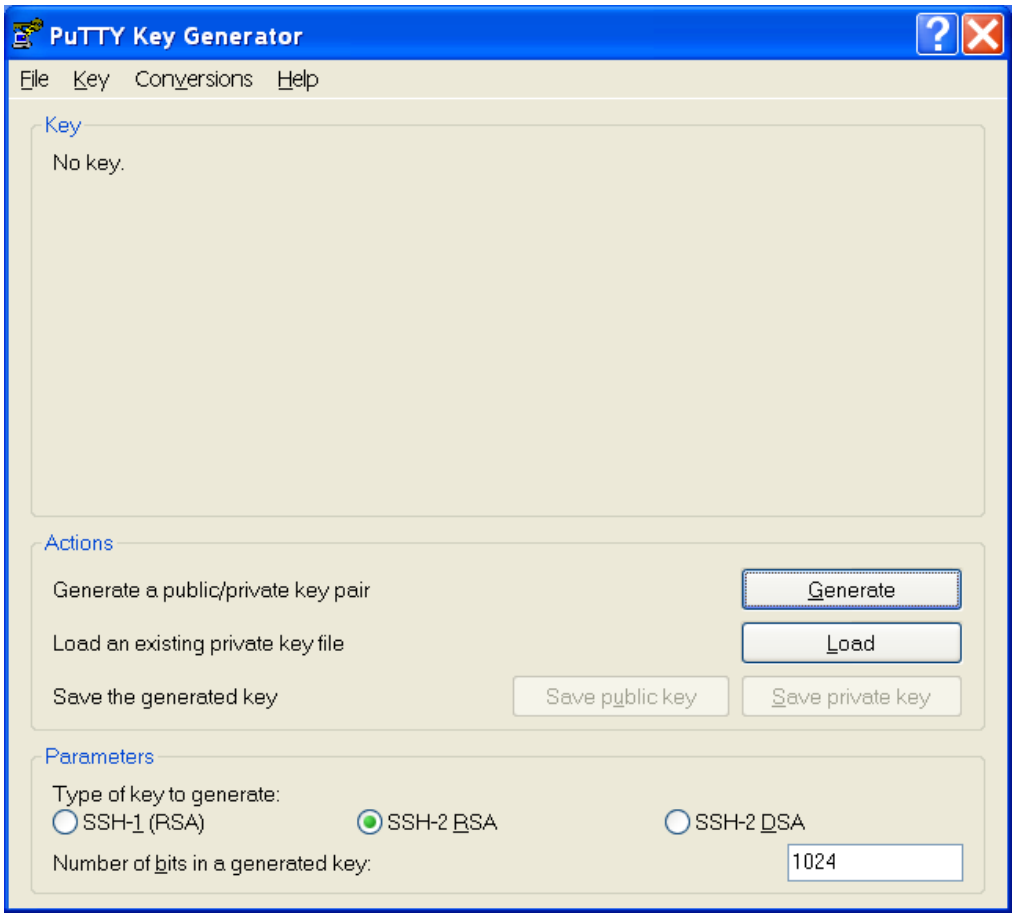
3.3.1 Using Microsoft® Windows 32 Bit Operating systems:

- **WinSCP**

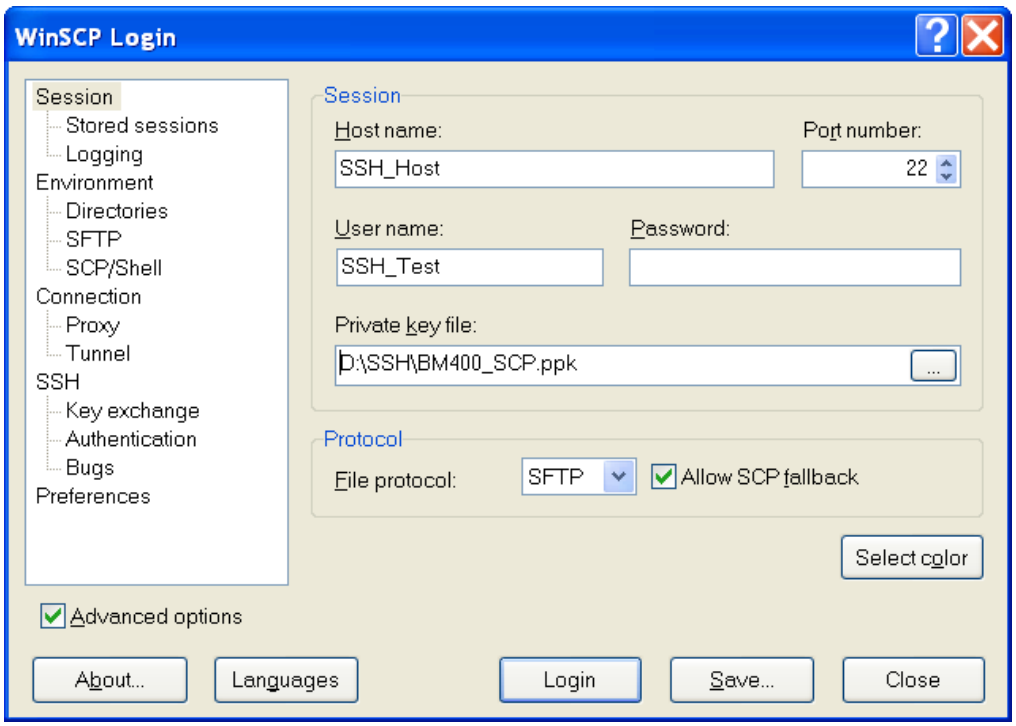
WinSCP is an Open Source client providing FTP and SFTP capabilities in combination with a Graphical User Interface to transfer and to download data to a SSH server. WinSCP also offers a Batch mode and a command line interface running in a DOS window with a command set comparable to those of a standard FTP client to transfer data.

Configuration:

Create a key pair using the program puTTYgen (Generate) and send the public part of the key to the *BusinessMail X.400* Administration who will store this key on the SFTP server systems. Store the private key locally to use with WinSCP.



Start WinSCP and create a new ‘Stored session’ by entering the Hostname (SFTP server name - DNS name) or the numerical IP address (provided by the *BusinessMail X.400* administration), the user name and the path to the “Private key file”.



Use the button „Login“ to log into the SSH server for the first time. While connecting to the SFTP server WinSCP will ask for the passphrase for the private key (can be imported via file in batch mode). With the first session the SFTP server will send his public key and you are prompted to accept it in order to continue the session.

In menu item „Preferences → other general options“ you can tailor WinSCP to your requirements.

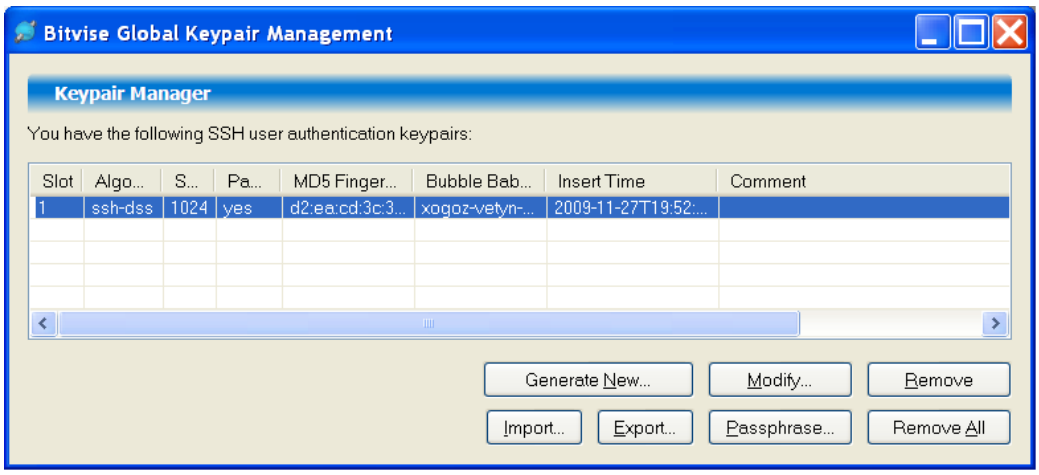
- **Bitvise SSH Client (formerly Tunnelier)**

This is a SFTP client that also offers a Graphical User Interface, Batch mode and a DOS command line mode. For smaller installations Bitvise SSH client is free - a right of use must be purchased if Bitvise SSH client is used by 5 or more people or on 5 or more machines -. Additional licenses have to be ordered.

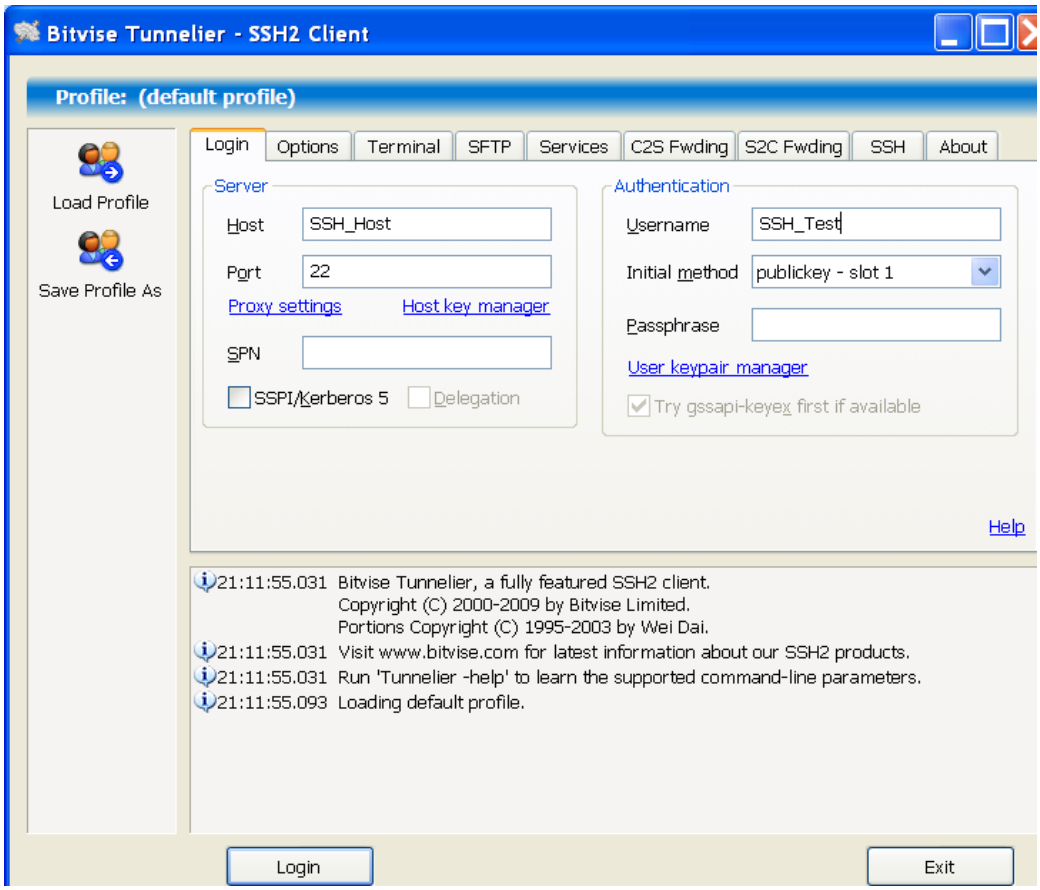
Compared to WinSCP the Bitvise SSH Client has a higher throughput and consumes less CPU time.

Configuration:

Create a key pair using the program Keypair Management (Generate New) and send the public part of key to *BusinessMail X.400* Administration where the public key will stored on SFTP server systems. Please verify that there is no space in the value of the comment field while creating the key pair because the Keypair Manager will export the comment without quotation marks into public key file. And so the SFTP host is not able to import this key.



Start Bitvise SSH Client to create a communication profile. Enter the name of the SFTP server system (DNS name) or the numerical IP address in the “Host“ field. In the field “Username“ use the username provided by the *BusinessMail X.400* Administration. In the field, “Initial method“ select the slot of the stored key and in the field “Passphrase” the password of the key.



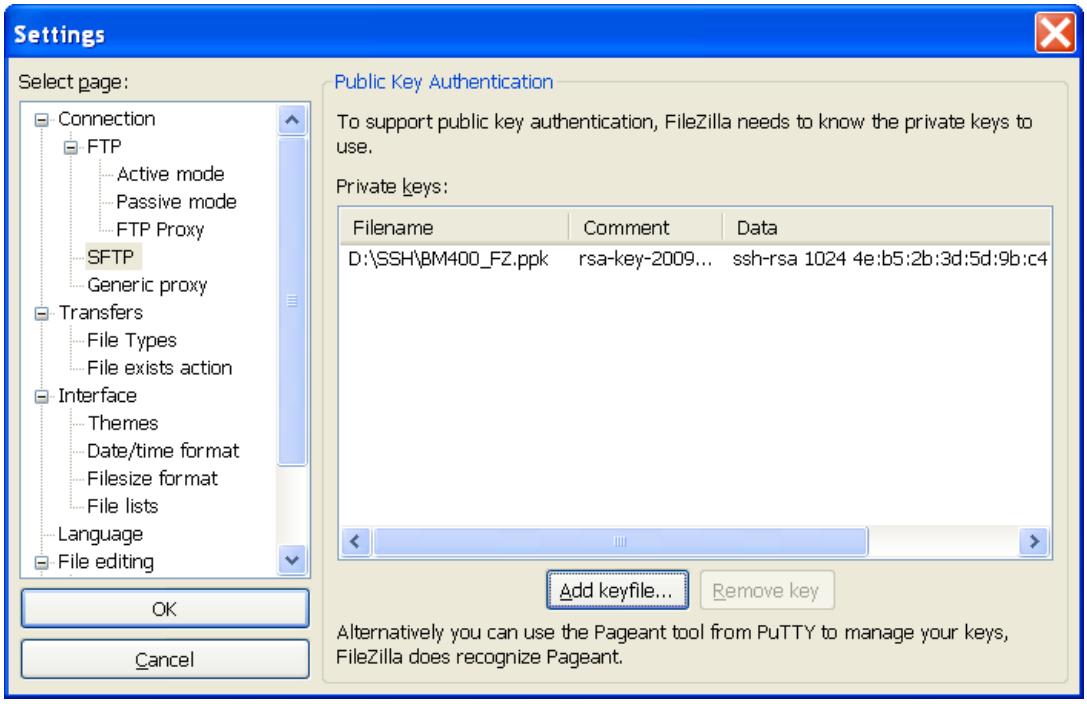
Under the “SFTP” tab the local directory displayed in the GUI can be configured. A SFTP session can now be established. When establishing a SFTP connection the key of the SFTP host has to be accepted.

- **FileZilla**

FileZilla is an Open Source client for FTP and SFTP comparable to WinSCP.

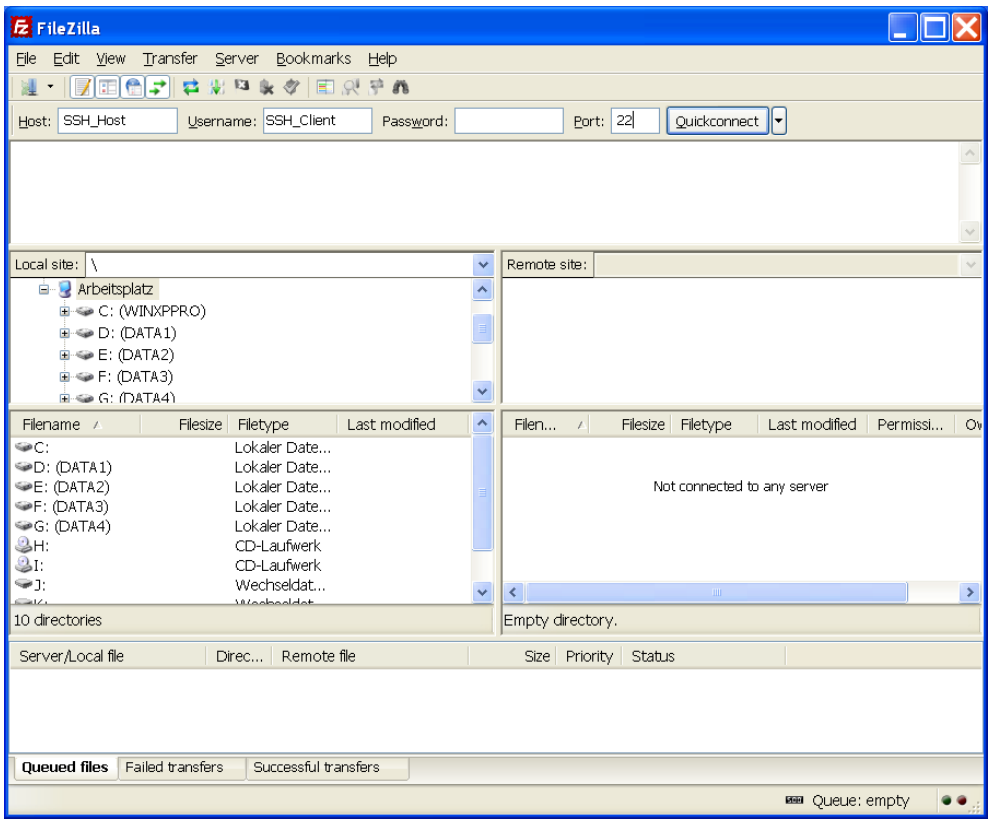
Configuration:

You need an appropriate tool (for example puTTYgen) to create a key pair (Generate) and send the public part of the key to the *BusinessMail X.400* Administration who will store this key on the SFTP server systems. The private key has to be stored locally (Settings → SFTP) for use in FileZilla.



Now you can configure the access to the *BusinessMail X.400* MessageGate directory. Enter the name of the SFTP server (DNS name) or the numerical IP address in the field “Host“ and the user name (provided by *BusinessMail X.400* administration) in the field “Username”.

During the first session you have to accept the key of SSH host.

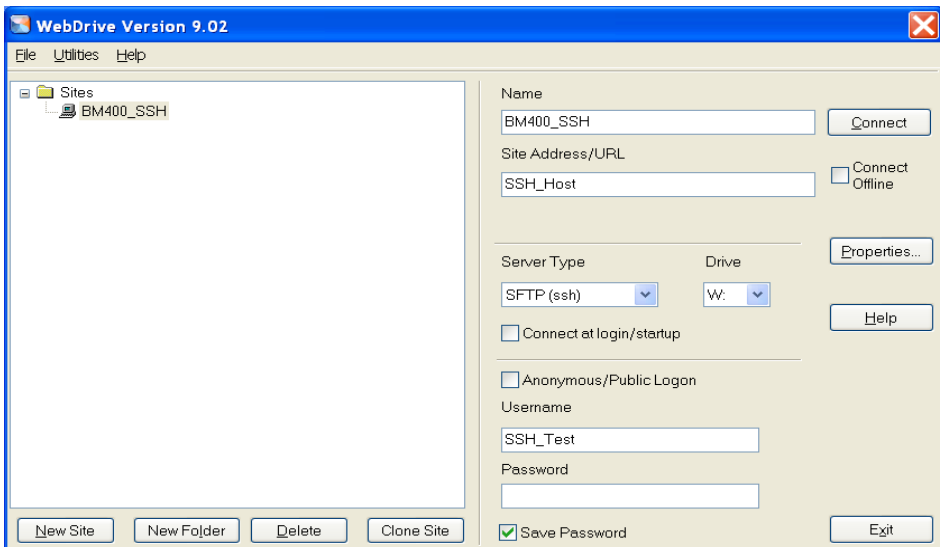


- **WebDrive produced by South River Technologies (topical Version 9.13)**

Creates a network drive and assign a local drive via SFTP (and also via FTP or WebDAV, see Chapter 4 Access via HTTPS/WebDAV to handle it as a local directory.

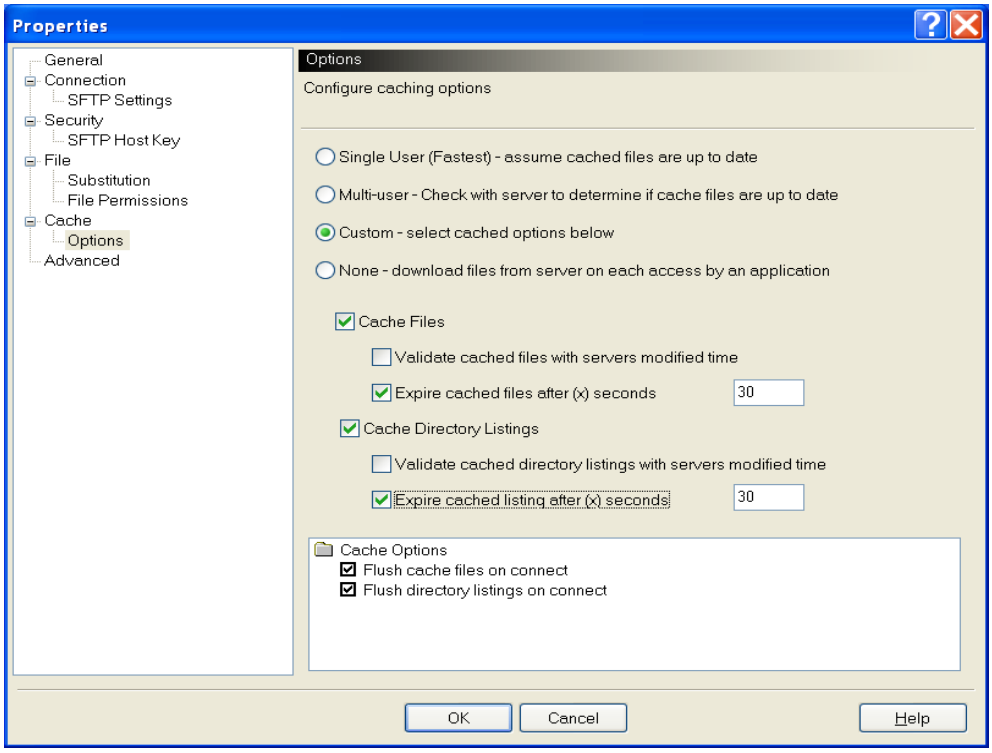
Configuration:

Create a key pair using the Host Key Manager (Utilities -> Host Key Manager) for example with RSA 2048 bit and store the public part of the key in a file and send this file to the *BusinessMail X.400* Administration who will store this key on the SFTP server systems.
Configure connection → Open WebDrive → New Site → Site Address/URL enter address of MessageGate directory and username (provided by *BusinessMail X.400* administration).

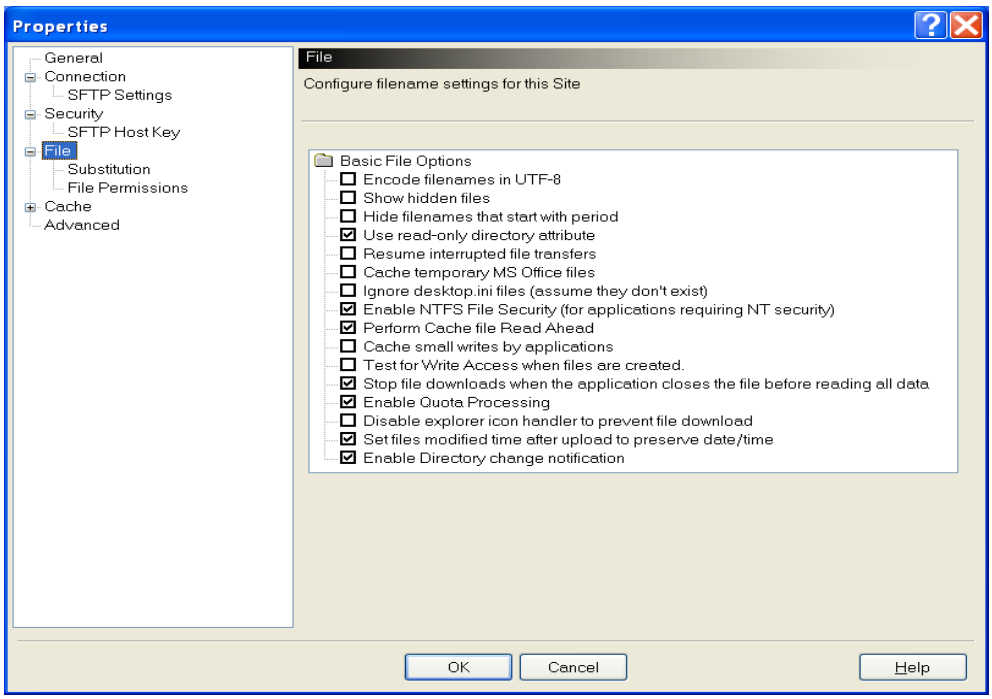


Assign certificate → Properties → Security → SFTP HostKey → choose Client Host Key und enter password.

Configuration Cache → Program Setting → Cache Settings → Options → Costum -> Expire cached files after 30 seconds and Expire cached listings after 30 seconds



Enable the option “Enable Directory change notification“ so that the client displays the files that MessageGate stores in the directory.



3.3.2 Microsoft® Windows 64 Bit Operating systems

All products described in the last Chapter will also run on Windows 64bit systems. **South River Technologies** WebDrive is also available as a native 64bit Version.

3.3.3 Linux and UNIX Operating system

- **SFTP as part of the OpenSSH suite**

A key pair using the program ssh-keygen needs to be created. For example the command “ssh-keygen –t rsa –b 2048” will generate a 2048 Bit RSA key to use with SSH V2. The key files id_rsa (private key) and id_rsa.pub (public key) are then stored in the hidden subdirectory “/.ssh” of the respective user directory. Before the user’s public key is sent to the *BusinessMail X.400* administration it needs to be converted using the following command:

```
# ssh-keygen -e -f ~/.ssh/id_rsa.pub > ~/.ssh/ssh_xxxxx.pub
```

where xxxxx is the User-ID of the MessageGate account. To connect to the SFTP host the following command is used:

```
# sftp username@ssh_host_name”
```
(username of the VMS account!).

During the first session the key of the SSH host needs to be accepted.

- **FileZilla**

FileZilla is an Open Source client for FTP and SFTP comparable to WinSCP.

Configuration:
The configuration of this client is equivalent to those of the Windows version (see Chapter 3.3.1). The newer versions of this client also include a key generator called fzputtygen.

3.3.4 Apple Mac OS X

- **SFTP as part of the OpenSSH suite using the terminal program**

The OpenSSH suite and the included SFTP client can only be run in the context of a terminal session. A key pair using the program ssh-keygen needs to be created. For example the command “ssh-keygen –t rsa –b 2048” will generate a 2048 Bit RSA key to use with SSH V2. The key files id_rsa (private key) and id_rsa.pub (public key) are then stored in the hidden subdirectory “/.ssh” of the respective user directory. Before the user’s public key is sent to the *BusinessMail X.400* administration it needs to be converted using the following command:

```
# ssh-keygen -e -f ~/.ssh/id_rsa.pub > ~/.ssh/ssh_xxxxx.pub
```

where xxxxx is the User-ID of your MessageGate account. To connect to the SFTP host use the command

`# sftp username@ssh_host_name”` (username of the VMS account!).

During the first session the key of the SSH host needs to be accepted.

- **FileZilla**

FileZilla is an Open Source client for FTP and SFTP comparable to WinSCP.

Configuration:
The configuration of this client is equivalent to that of the Windows version (see Chapter 3.3.1). The newer versions of this client also include a key generator called `fzputtygen`.

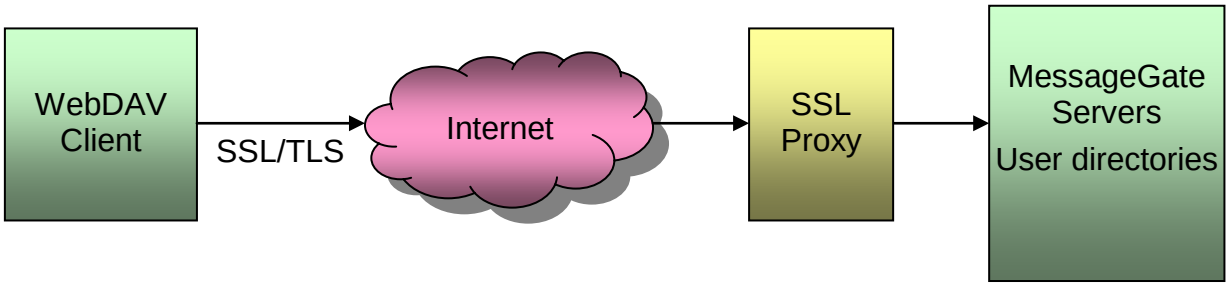
3.3.5 Other operating systems

There are ports of the OpenSSH suite available for the IBM operating systems *i5/OS* now called *IBM i* for Business and *zOS* so the description in Chapter 3.3.3 Linux and UNIX Operating system should also apply to these operating systems. However these assumptions cannot be verified, as these operating systems are not available in the test environment.

4 Access via HTTPS/WebDAV

4.1 General

An alternative to the SFTP access described in the last chapter is the access via https with WebDAV extension. HTTPS/WebDAV is the recommended communication protocol for those customers using Internet to access their MessageGate directory. Only connections using SSL/TLS (min. 128 Bit key length, server supports 256 Bit AES) via the Internet will be accepted. The HTTPS/WebDAV access provides comparable functionality to the FTP command set but with the inherent advantage that it does not require two TCP/IP (Management and data) channels for a session. For many customers access via WebDAV provides a better security concept/ rule (Firewall, Proxy etc.) than FTP. In addition WebDAV provides the inherent advantage that remote disks on the WebDAV server system appear to an application as local disks. Hence the application does not have to be specically adapted to provide the communication environment. This can be provided by a separate component.



To access the directory use the following URL:

https://webdav.viat.de/~00000nnnnn/

where nnnnn is the User-ID (*BusinessMail X.400* internal identifier of an user account). The forward slash “/” at the end of URL is necessary otherwise the connection will fail.

To establish a SSL/TLS connection to the application server it is necessary that the WebDAV client sends a client certificate in response to the SSL proxy request. *BusinessMail X.400* will make this certificate available for the MessageGate/ WebDAV account configuration (PKCS12 file and a separate certificate and key file using PEM format). Using *WebConfig* (*see also Chapter 2.8 Communication and Trading Relation Profile*) download this certificate in the menu item “WebConfig Management”. This downloaded certificate has to be imported into the certificate store of your WebDAV application. By default there is a passphrase configured for the private key (see the text file associated with the certificate) because most existing WebDAV clients request a passphrase. If you are using a WebDAV solution that has problems using passphrases then please make *BusinessMail X.400* administration aware of this issue when you request your new account. In such cases a certificate can be generated without a passphrase. Please be aware that not all WebDAV solutions support the use of Client certificates. Chapter 4.3 contains information about successfully tested client solutions and associated libraries, which support Client certificates.

When configuring the MessageGate directory there is a choice to use this this client certificate also for the authentication to directly access it or an user name and password will be prompted and verified.

4.2 Features to note

Customers who only want to receive/fetch messages do not need a communication module that supports the WebDAV protocol. These files can be downloaded using a standard Web browser. The messages/data delivered to the file interface are purged automatically based on a pre-configured purge time. Customers who need to send messages require a separate WebDAV solution.

A customer who orders MessageGate with reduced functionality will only recognize that a message has been refused (in conjunction with the central EDI function) if the automatically generated status report is configured in the host profile or if a status report request has been configured via *WebConfig*.

Thefollowing sections include information about a selection of communication modules with which MessageGate access has been successfully tested.

See also the description of an Open Source Client, developed for Ruby and available on different OS platforms; in Chapter 8.3 Open Source Client for MessageGate.

4.3 Recommended WebDAV Clients

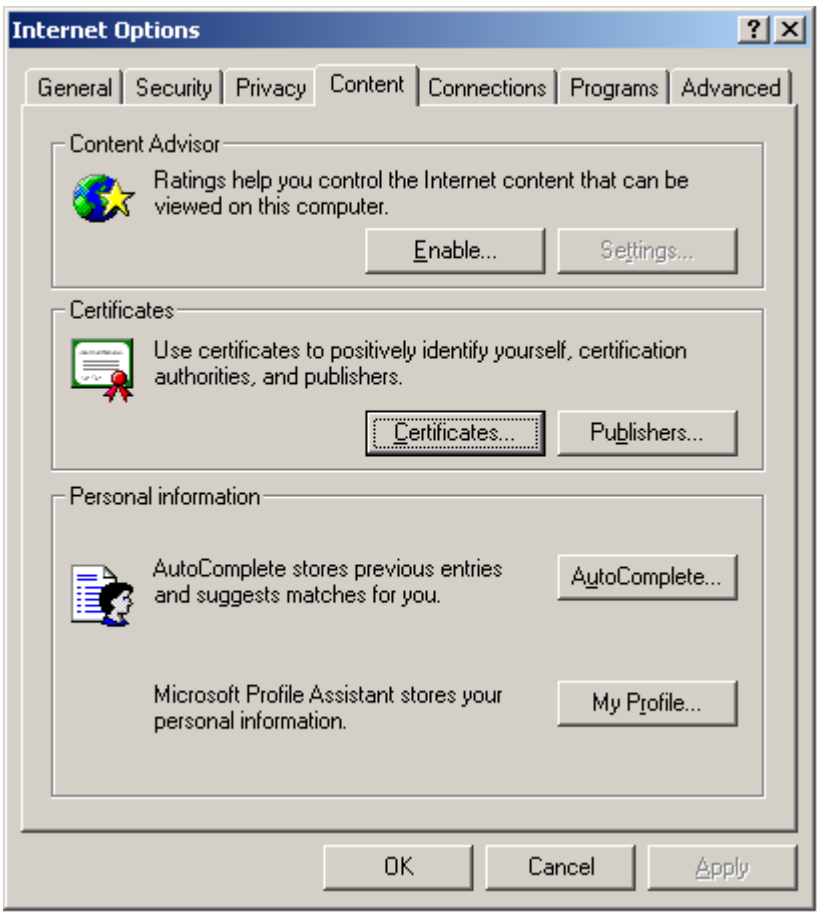
4.3.1 Microsoft® Windows 32 Bit Operating systems

- **Microsoft® Windows Explorer (Windows 2000 and newer)**

Configure a new Web Folder in my Network place.
When using Windows 2003 Server and IE7.0 or Windows Vista you may need to install the Patch KB907306 otherwise the connection can fail. In Windows 2003 Server you may also have to start Web client service because this service is set by default to “manually”. At the moment it is not possible to configure net drives using Windows 7 or Windows 2008 server because the authentication method of Web server is not compatible.

Configuration:
My Network place → Add a network place → https://webdav.viat.de/~00000... /

Requirement: Import certificate (*.p12) in Windows certs store → IE Explorer → Tools → Internet options → Content → Certificates → Import

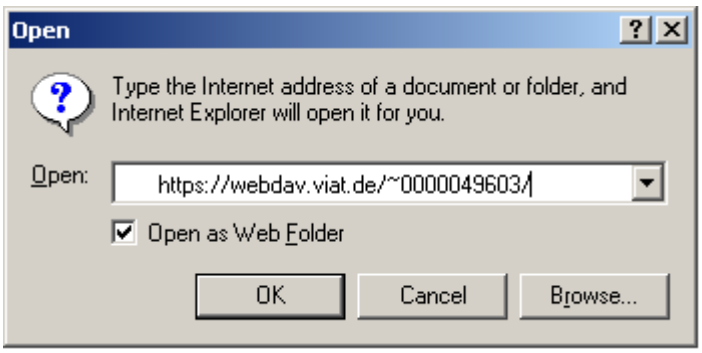


- **Microsoft® Internet Explorer (IE 6.0 SP1 or 7.0)**

When using Windows 2003 Server and IE7.0 or Windows Vista you may need to install Patch KB907306 otherwise the connection can fail. In Windows 2003 Server you also have to start Web client service because this service is set by default to “manually”. IE 8.0 does not offer this option.

Configuration:

Open → File → Open → Open as Web Folder → https.//webdav.viat.de/~000…/ while using the address described in Chapter 4.1.

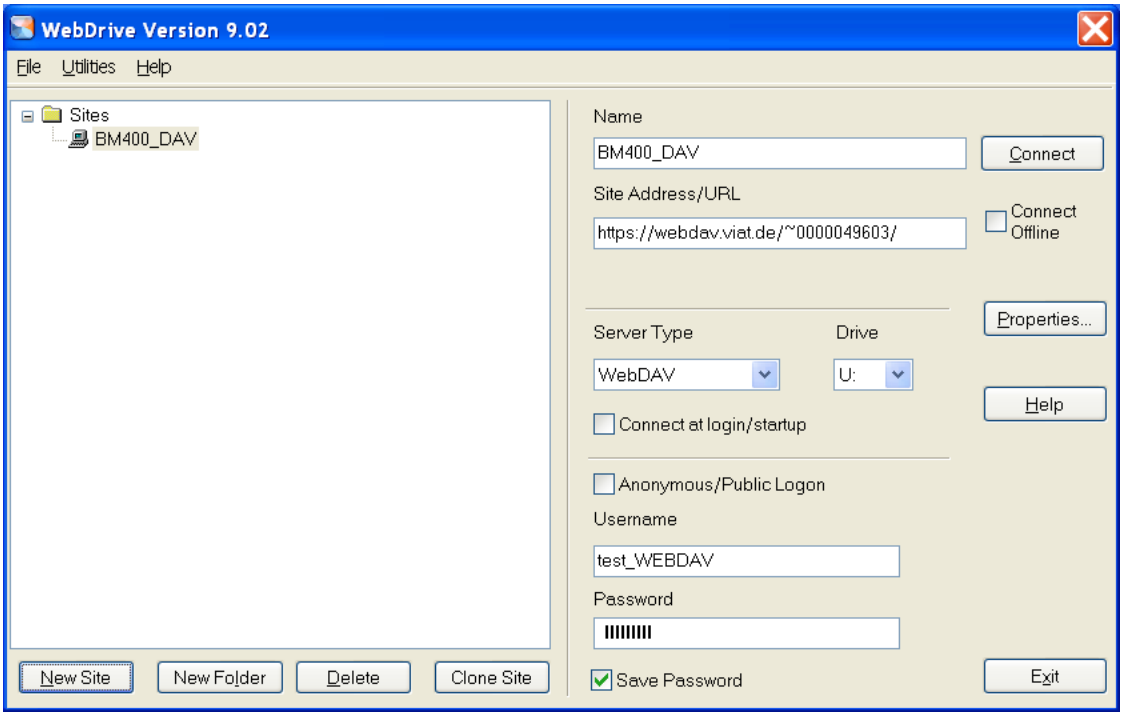


Requirement: Import the certificate (*.p12) into the Windows certs store (see Windows Explorer).

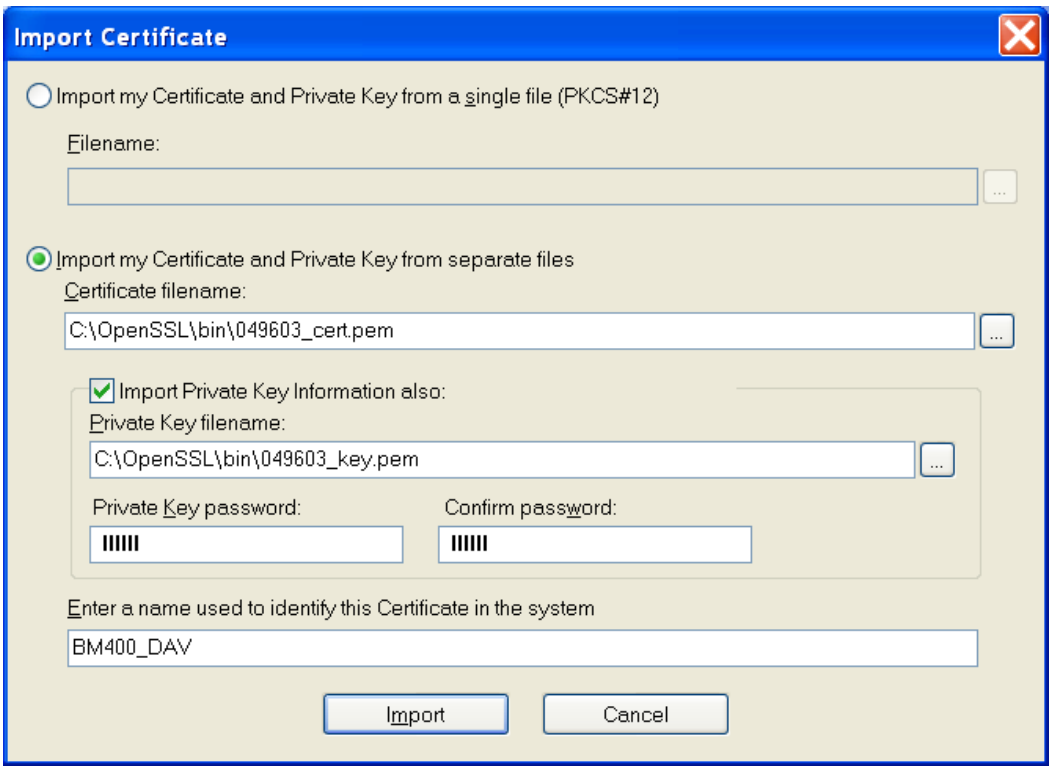
- **WebDrive produced by South River Technologies**

Creates a network drive and assigns a local drive via WebDAV (and also via FTP or SFTP) to make the remote directory appear as a local directory.

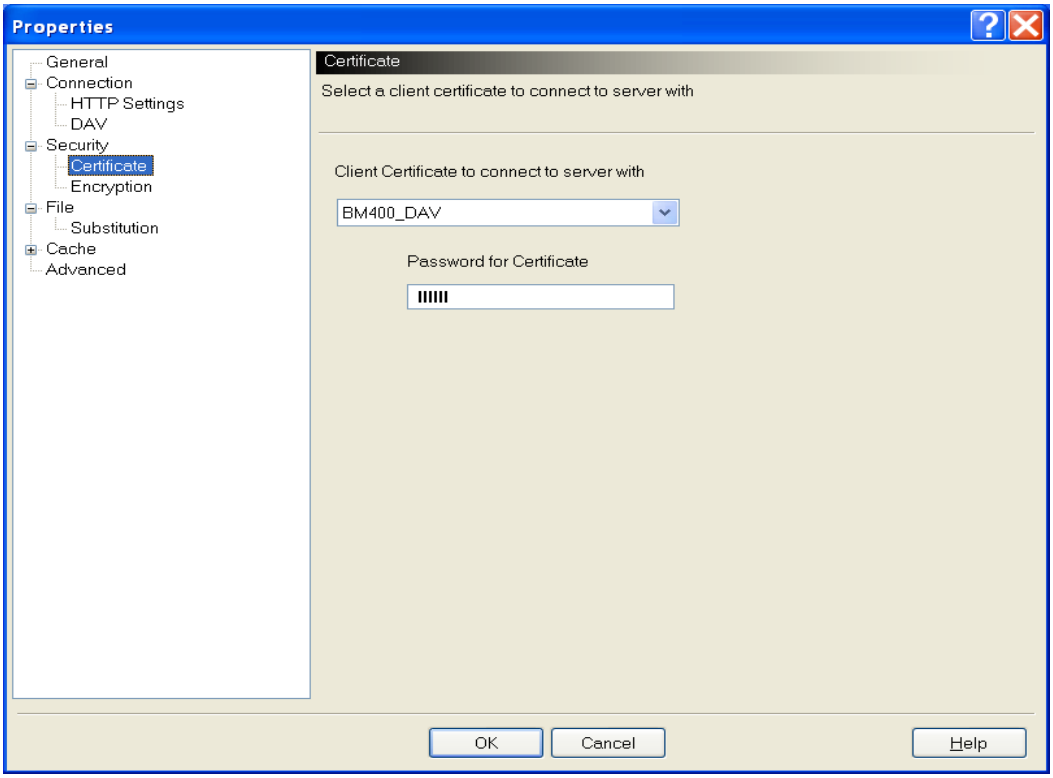
Configuration:
Configure connection → Open WebDrive → New Site → Site Address/URL enter address of MessageGate directory, and for the Username and Password fields provide the login values supplied by the *BusinessMail X.400* administration.



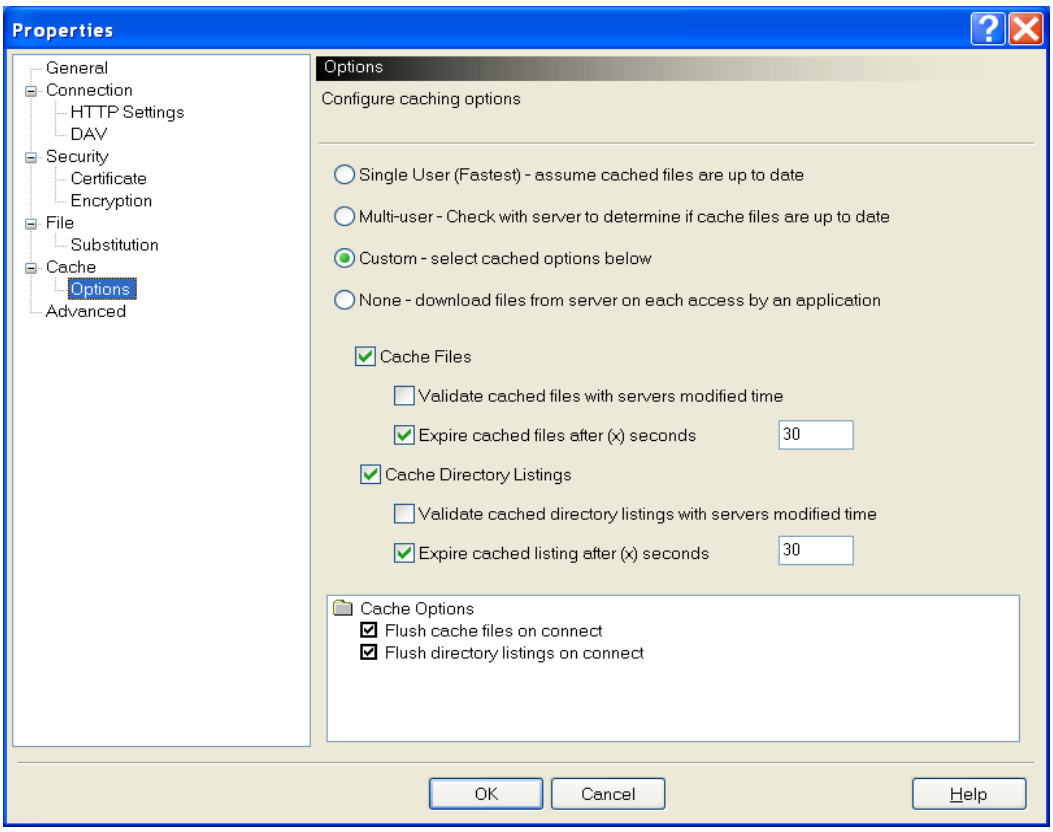
Import of certificate → Program Settings → Certificate Management → Certificate Manager → Import → Import from separate files: enter certificate and key file and password and assign a name for this certificate



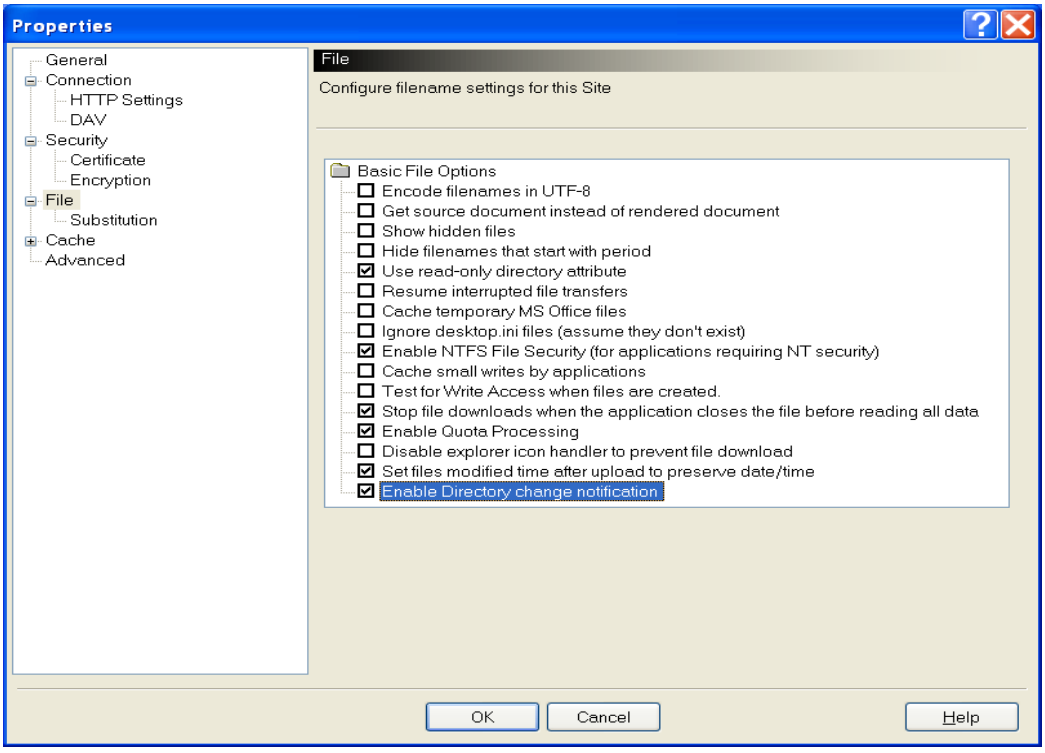
Choose certificate in Properties of site (Security → Certificate)



Configuration Cache → Program Setting → Cache Settings → Options → Custom → Cache File expires after 30 sec., Cache Directory Listings expires after 30 sec.



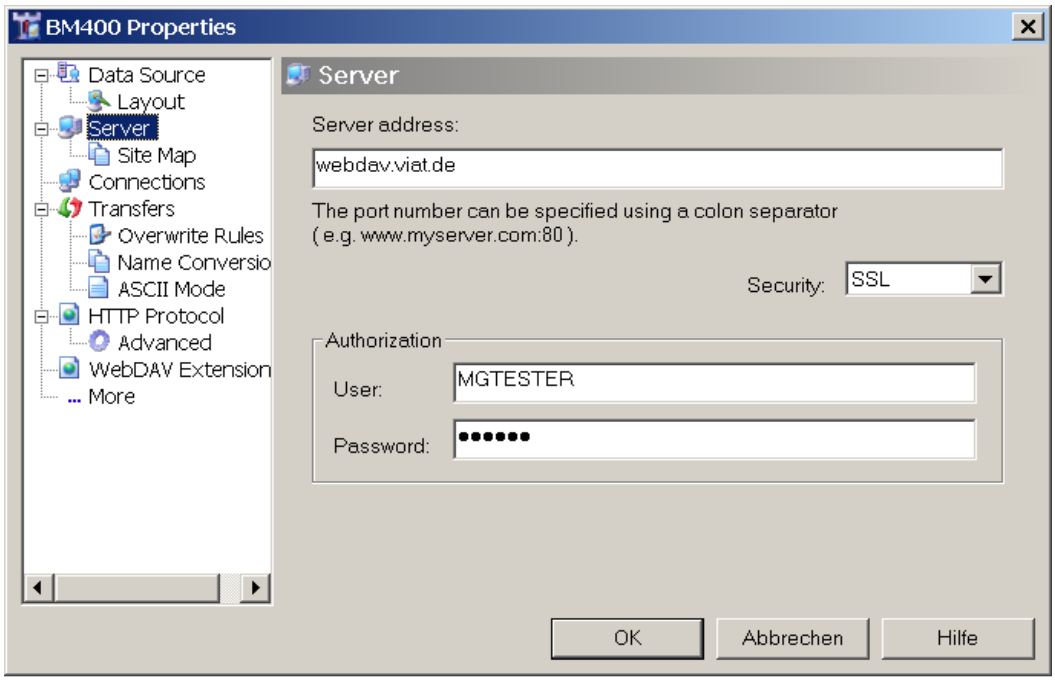
Enable the option “Enable Directory change notification“ so that the client automatically display the files that MessageGate places in the directory.



- **BitKinex produced by BARAD-DUR, LLC.**

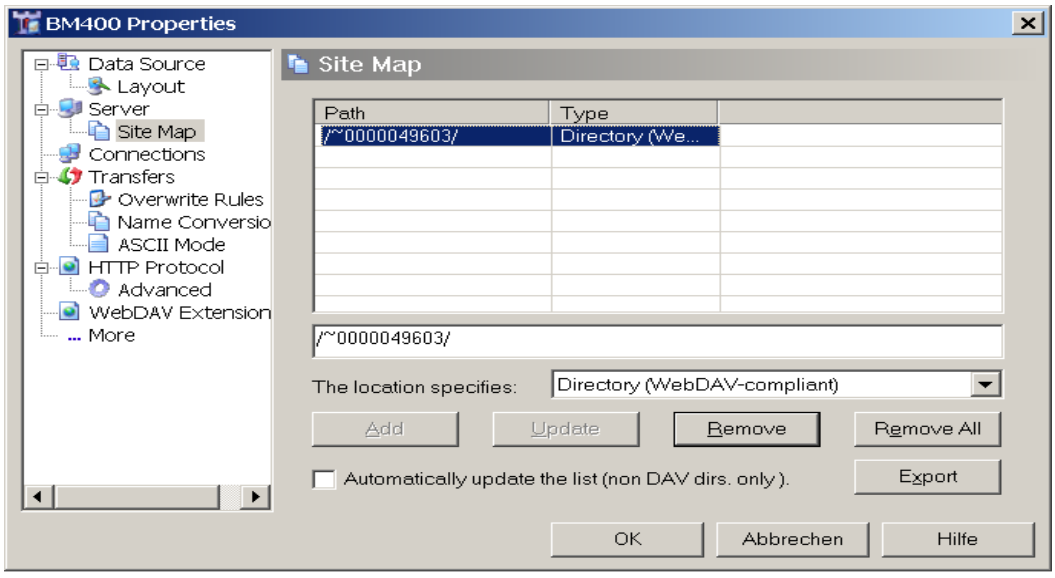
WebDAV Client (also supports FTP) provides Graphical User Interface and a Batch mode option.

Configure connection → Select http → Right mouse click or Data Source → New → http/webdav → Assign name→ Properties → Server



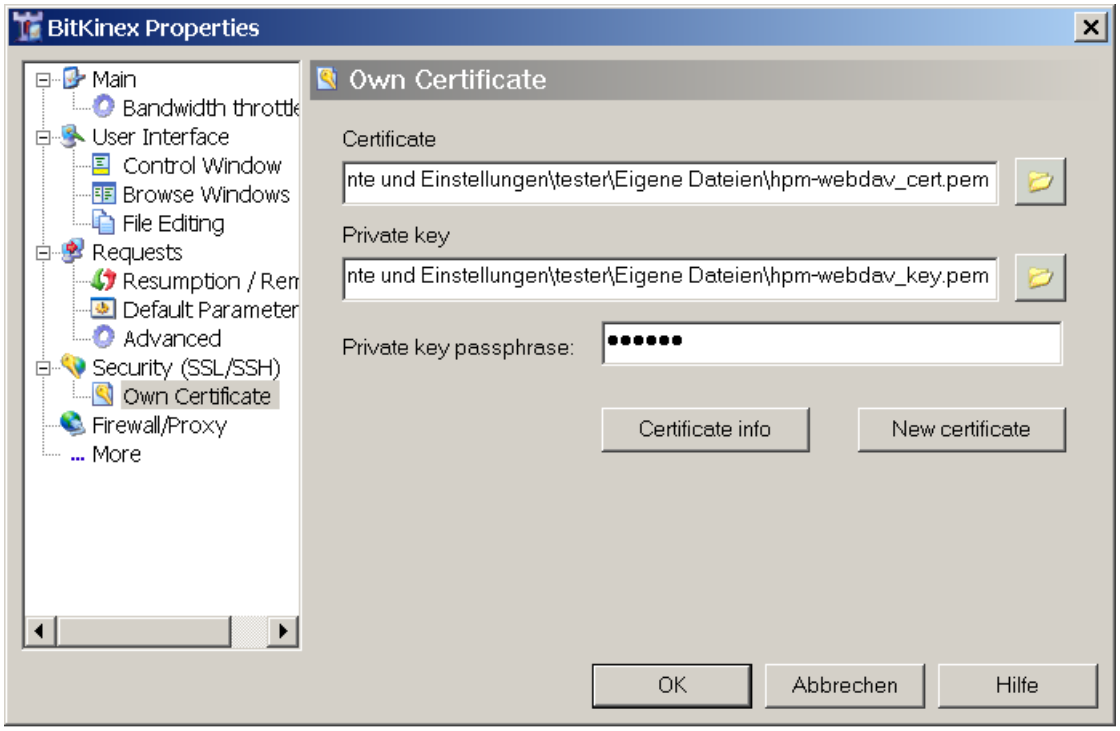
Server address: webdav.viat.de
Security: SSL
User + Password: Provide login data

→ Site Map



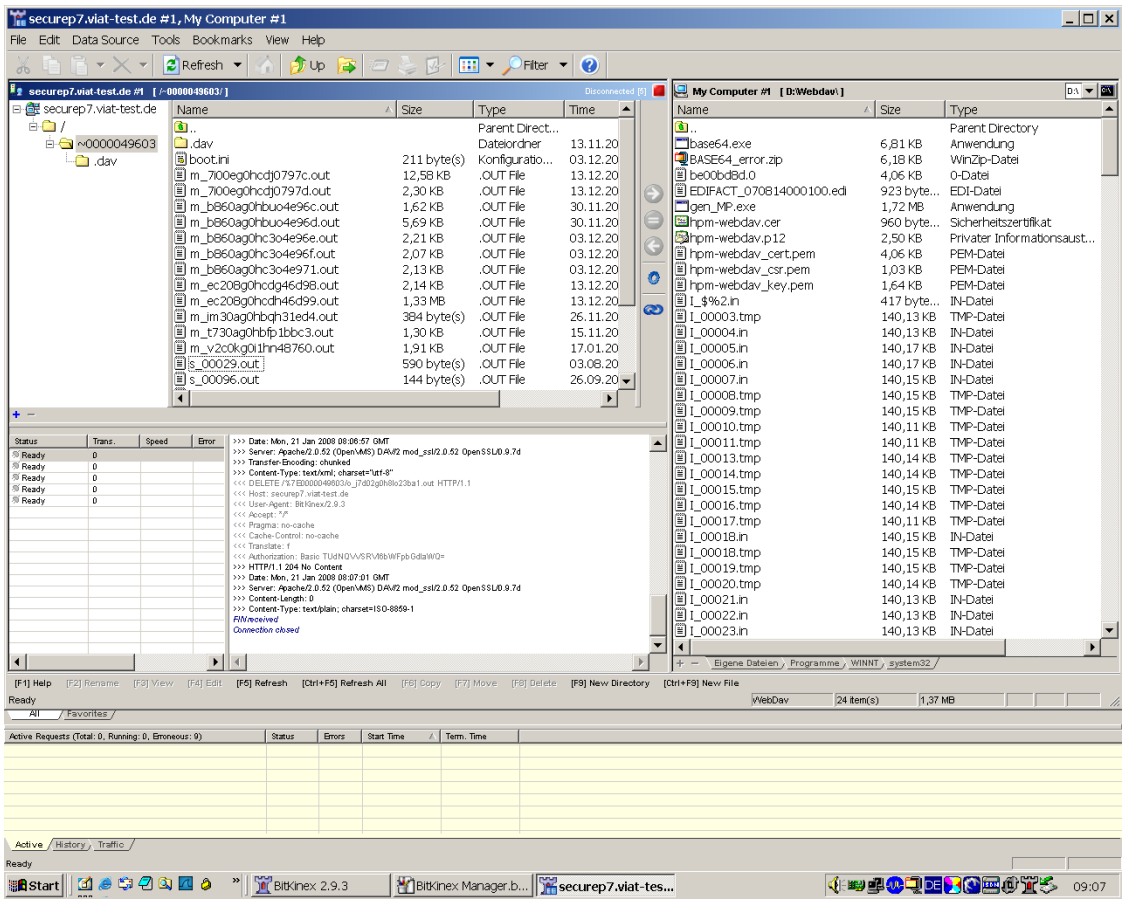
Path: /~00000nnnnn/ → (nnnnn is User-ID)

Configure certificate → File → Option → Security → Own certificate



Extract certificate and key file from the archive and enter the path for both files and the passphrase for the key file.

Double-click on the host entry to open Bitkinex FileManager.



Bitkinex also provides a command line mode (no GUI) so it would be possible to integrate the module into existing EDI solutions.

- **Mozilla Firefox 3.0.x for Windows with Add-on „Open as Webfolder 0.22“**

The Add-On “Open as Webfolder“ uses the Windows Explorer functionality to upload files to MessageGate and to delete files in the directory. The better approach would be to use Windows Explorer directly. There is no WebDAV Add-On for the Linux version of Firefox.

- **Onion (WebDAV C++ Library)**

There is no active support for this library at the present time.

- **Neon (WebDAV C Library, most WebDAV Clients were developed based on this library)**

Library is updated frequently.

4.3.2 Microsoft® Windows 64 Bit Operating systems

All products described in last sections will also run on the 64bit Windows. South River Technologies also offers WebDrive as a native 64bit version.

4.3.3 Linux and UNIX Operating system:

- **Cadaver**

Cadaver is command line based Client which provides almost the same functionality (commands, syntax) as provided in FTP command line based Clients for Linux and Microsoft® Windows.
One has to first import the client certificate using the command “set client-cert certifikatename.p12”. When connecting to MessageGate the Cadaver Client initially prompts for the certificate passphrase. Consider obtaining a certificate without a passphrase from *BusinessMail X.400* administration.

- **Konqueror (Web und Directory Browser for Linux)**

Assign address „webdavs://webdav.viat.de:443/~xxxxxx“.
In older Linux versions you may encounter problems with IP V6 support. If this is the case you should disable this feature.

Configuration:
Requirement: Import client certificate in Setting → Configure Konqueror → Encryption → Your certificate.
You now have to configure this certificate to be the default or select that Konqueror always prompts for a client certificate.

Newer Linux distributions (SuSE and 9.3 and newer) include features to configure a web folder using Konqueror.
In SuSE Linux select Network browser → Add network folder → Web folder:

- Enter a name for this folder
- Enter the username of your WebDAV Accounts
- Enter server „webdav.viat.de“
- Enter Port 443

- Enter folder „~00000nnnnn“ where nnnnn is User-ID of your MessageGate Account
- Encrypt session

- **DAVfs (File system for Web folders based on WebDAV protocol)**

Installation kit for Debian and Ubuntu but after installation the required libraries DAVfs will also run on SuSE Linux.
Required libraries DAVfs will also run on SuSE Linux.
For a separate installation description see *http://www.service-viat.de*
Please be aware that the file system has to be unmounted before a server shutdown!

- **Sitecopy (Program to map the content of local directory into MessageGate directory and vice versa)**

Starting Version 0.16.3 the configuration might be:

```
***
site webdav
server webdav.viat.de
protocol webdav
username <Username>
password <Password>
client-cert </path/to/cert.p12>          #in man-page not listed!
remote /~<User-ID>/
local /<localer/pfad>/
http secure
```

- **Onion (WebDAV C++ Library)**

There is no active support for this library at the moment.

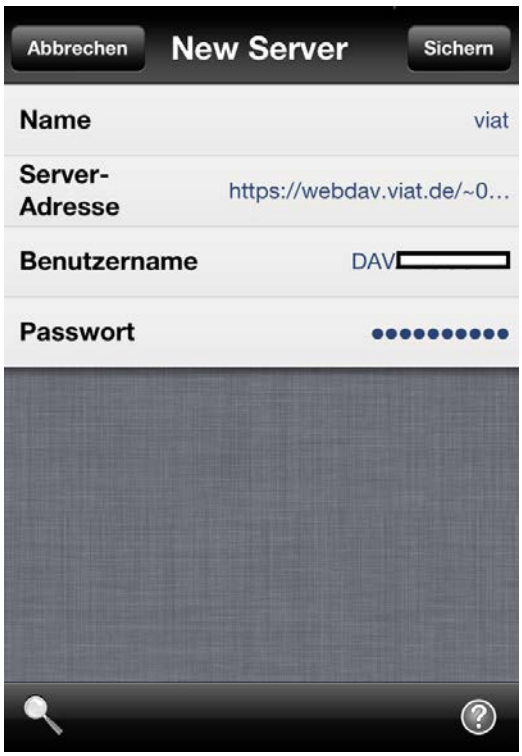
- **Neon (WebDAV C Library, most WebDAV Clients were developed based on this library)**

Library is updated frequently.

4.3.4 Apple iOS

- **WebDAV Nav+ (commercial App for power user, the free version WebDAV Nav does not support the use of a client certificate)**

Use the iPhone App Store to download and install the app. A new profile using the login values supplied by the *BusinessMail X.400* administration needs to be created.



Next the PKCS12 file for the authoritzation of the connection for the SSL proxy needs to be placed in the root directory using the name of the profile. In our example this would be the file name „viat.p12“.

Now you should be able to log into your MessageGate directory and to upload or download files. The following picture shows the available options.

4.3.5 Other operating systems

- **Neon (WebDAV C Library, most WebDAV Clients were developed based on this library) available for Unix OS**

Library is updated frequently

- **Sitecopy (Program to map the content of local directory into MessageGate directory and vice versa)**

Starting Version 0.16.3 the configuration might be:

```
***
site webdav
server webdav.viat.de
protocol webdav
username <Username>
password <Password>
client-cert </path/to/cert.p12>          #in man-page not listed!
remote /~<User-ID>/
local /<localer/pfad>/
http secure
```

5 AS2 and MessageGate Process

5.1 General

The AS2 Gateway users are not aware that they are using a MessageGate process because the AS2 communication is serviced by a module called ComAS2 (Java communication module offered by Compinia GmbH & Co. KG for different Operating systems, e.g. Windows and Linux). The MessageGate process (MGAS2X) accepts AS2 documents received via ComAS2, creates X.400 messages and send these to the respective partners. X.400 messages destined for an AS2 user are forwarded directly by MessageGate to ComAS2. ComAS2 in turn transfers these documents using EDIINT AS2 protocol to the configured URL of the user's application. MessageGate also maps X.400 reports to AS2 MDN and vice versa. Depending on the configured gateway mode the AS2 MDN will be mapped into X.400 Receipt Notification or X.400 Delivery Notification.

Gateway-Modus „Agent" or „Transfer"

If the gateway mode is "Agent" (Default) MessageGate will send a requested X.400 Delivery Notification (DN) when message was provided to the AS2 communication module (ComAS2) for delivery to the customers AS2 solution. A MDN sent for this delivery would be mapped into a Receipt Notification (Read Notification → Status in Report is „Read") if requested by the X.400 partner and enabled by the AS2 user. If the gateway mode is "Agent" the AS2 user has the access to several useful features in *WebConfig*, e.g. Overrun and automatically generated Status report.

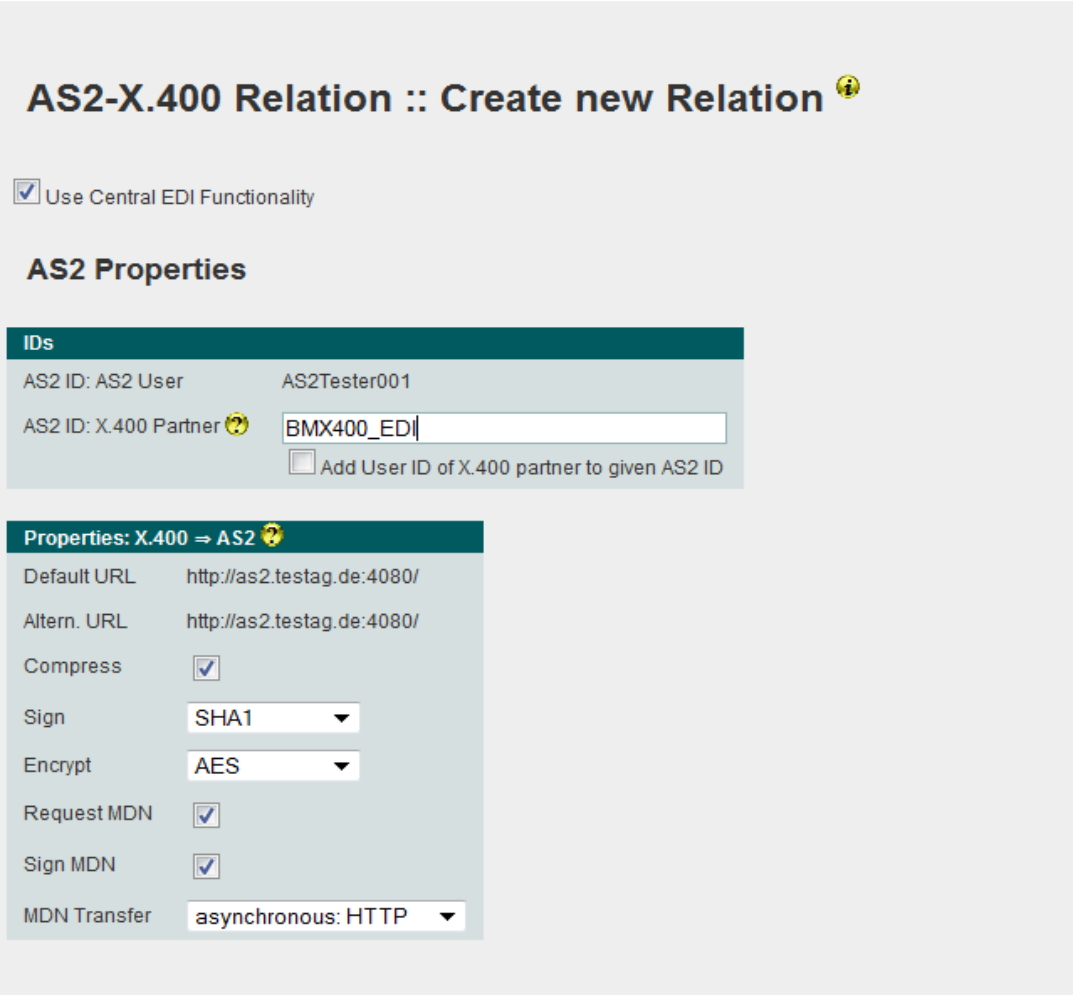
The gateway mode "Transfer" should be used if the AS2 user is not a customer of *BusinessMail X.400* and such does not have the ability to use *WebConfig* and the extended features of the AS2 gateway. In this case the X.400 user orders and pays for the AS2 connection. For this X.400 user it is important that the MDN sent by the AS2 partner will be mapped into a Delivery Notification (Status in Report is „Delivered"). A requested RN will be ignored and the Overrun functionality is disabled. While using gateway mode "Transfer" the X.400 Standards will define the message expiry time out values and a NDN with appropriate error code will be send for expired messages.

Both ComAS2 and MessageGate support the MIME content type "Multipart mixed".

While using the *BusinessMail X.400* AS2 Gateway an AS2 user's X.400 partners always appear as AS2 partners and vice versa, an X.400 user's AS2 partners appear as X.400 partners without any restrictions with regard to the respective transport protocol used.

EDIINT AS2 (RFC4130) is a Peer-to-Peer protocol so that the AS2 user has to assign a separate AS2 ID for each of his partners. If he wants to communicate with X.400 partners via the AS2 Gateway he also has to assign AS2 IDs for these partners. This AS2 ID will be mapped in the AS2 Gateway based on the host trading profiles to the X.400 address of a partner and this address will be used when sending X.400 messages.

An AS2 user can also use the *BusinessMail X.400* central EDI functionality to send EDIFACT documents to X.400 partners or to receive EDIFACT documents when configuring a trading relation and assigning an AS2 ID for the central EDI function.



In such a case the AS2 user will only need one AS2 ID to communicate with several X.400 partners because the central EDI function will use the header information in the EDIFACT documents to find the partner's X.400 address. This option can help the AS2 user to reduce the costs if the AS2 application has a per partner license model.

Please be aware that there is a feature to note in the central EDI functionality of AS2 Gateway that causes a difference to MessageGate or EDIBOX (special mailbox type) behaviour. It is possible to send a Transmission Set file including several EDIFACT interchanges but in this case the AS2 Gateway is not able to send a MDN based on DN or RN. Each interchange will result in a separate X.400 message so that the mapping of reports is not possible. The AS2-Gateway will send the MDN after the EDI function had processed all interchanges (sent the messages via MTA or refuse them in case of missing relations or wrong parameters). So use a Transmission Set file that includes only one EDIFACT interchange if you need the correct mapping of reports.

The MessageGate process also adds the X.400 addresses in the TO: and FROM: elements of the AS2 MIME Header. These elements are not necessary in the AS2 communication where AS2-TO: and AS2-FROM: are used to define recipient and sender. However in conjunction with the central EDI functionality it is these elements that provide the AS2 users with information about the sender of the EDIFACT document.

5.2 Differences between File Interface and AS2 users

The following pages describe an AS2 account configured to run in the MTA mode “Agent” where the AS2 user has access to *WebConfig*. In the MTA mode “Transfer” the menu items EDI relations, Overrun and automatically generated Status report will not be available or the access will be restricted. By default, in the MTA mode “Transfer” there will be only one relation between an X.400 user who is a customer of *BusinessMail X.400* and his partner using an application that only supports AS2 and who is not a customer of *BusinessMail X.400*.

For the mapping between MDN and X.400 Reports and vice versa the Message-Gate process uses the same database relation (Trace_Tab) to store the message status information. An AS2 user can also request a Status Report in the *WebConfig* GUI (View/Download) or configure the delivery of Status Reports via the AS2 protocol from a preconfigured AS2 ID process (for more details about the format of the entries see the end of this chapter).

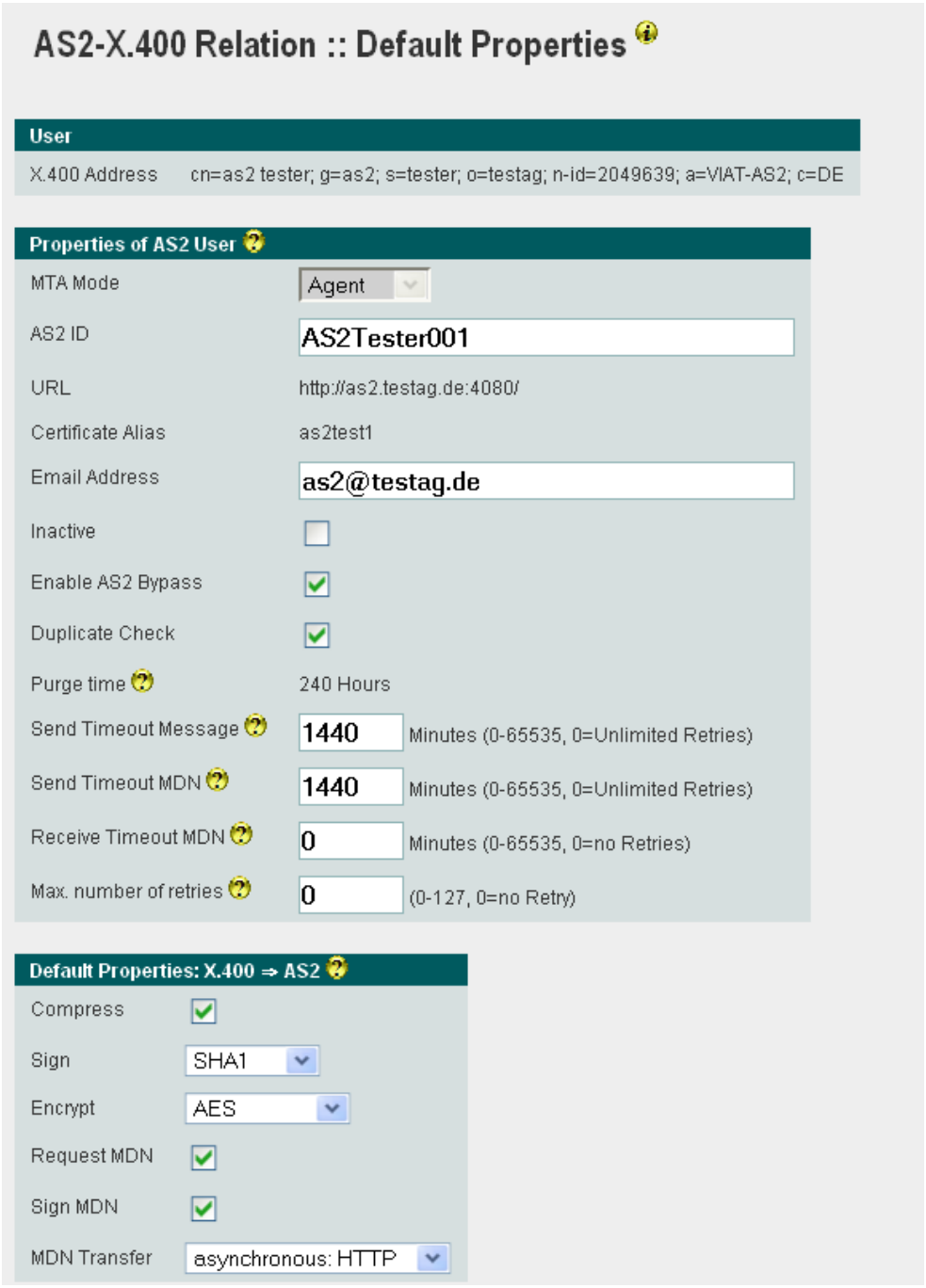
The MessageGate process will not delete the database entries once the transaction (data transferred and report sent) is completed. The entries will remain in the database until the end of the entry lifetime (determined by the purge time). The *“Purger”* process runs several times a day and deletes the entries that have reached the end of their lifetime (default is 240 hours = 10 days, this can be configured individually on customer request).

If the *“Purger”* process deletes an entry of a transaction that has not yet completed (for example a requested RN has not yet been received and ComAS2 has not been able to send an asynchronous MDN) the final status will be set to “failed”.

Properties of AS2 communication

The mapping between X.400 and AS2 messages (data compression, signing, encrypt message, request MDN) and between the reports is configured in the *WebConfig* menu item “AS2 – X.400 Relation: Default Properties” or in the Trading Relations.

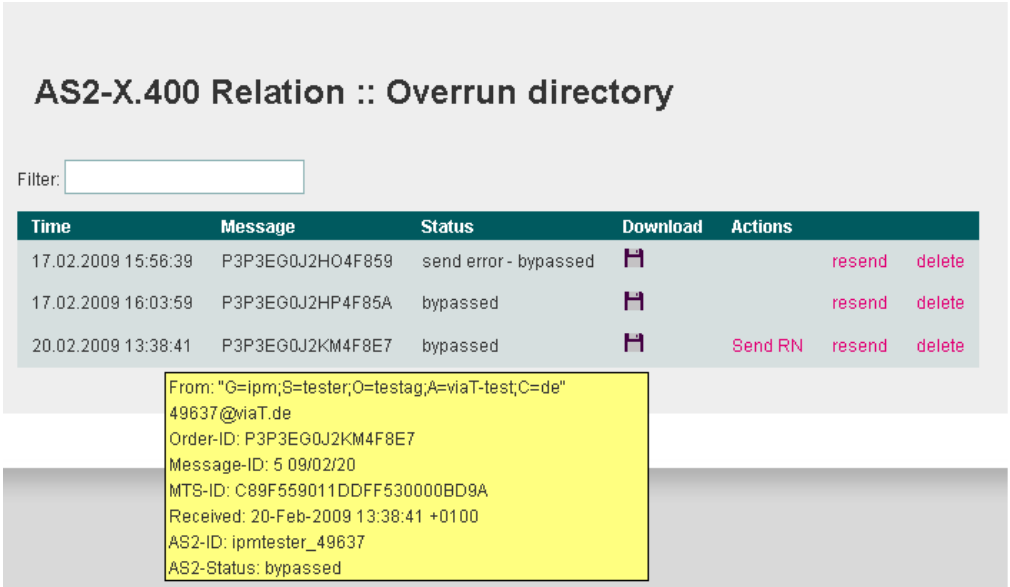
There are some other additional options configured in “Default Properties”.



Send Timeout of an AS2 message

Apart from the configuration of the AS2 ID and the URL of his AS2 application the customer can define how the AS2 Gateway should react if problems occur when delivering messages or reports to the customer's application. One can configure how long the AS2 Gateway should try to deliver a message before moving the data of this transaction into the Overrun directory for manual intervention. A user can manage the entries in his Overrun directory using *WebConfig* to either download the message user data, delete it or to reactive the transaction.

Overrun



The entries in the Overrun directory are available until the “Purger” process deletes them in the database relation (Trace_Tab). If a message stored in the Overrun directory had been reactivated, the AS2 Gateway will try to deliver it if the switch “AS2 Bypass” is still enabled. In such a case the message will only be moved into the Overrun directory if the send timer has expired.

Send Timeout MDN and retransmit AS2 message

The parameter “Send Timeout MDN” defines how long the AS2 Gateway will try to deliver an asynchronous MDN to a user’s AS2 application before it will set this transaction status to “failed”.

The next two parameters define whether the AS2 Gateway should retransmit a message if the requested asynchronous MDN has not been received in time (parameter “Receive Timeout MDN”) and how often the AS2 Gateway should retransmit the message. If the parameter “Max number of retries” is set to “0” the AS2 Gateway will directly move the message into Overrun directory after the Receive Timeout MDN timer has expired. If the parameter “Max number of retries” value is not “0” the AS2 Gateway will resend message as often as defined and then move the message into the Overrun directory.

Management AS2 communication in case of a problem

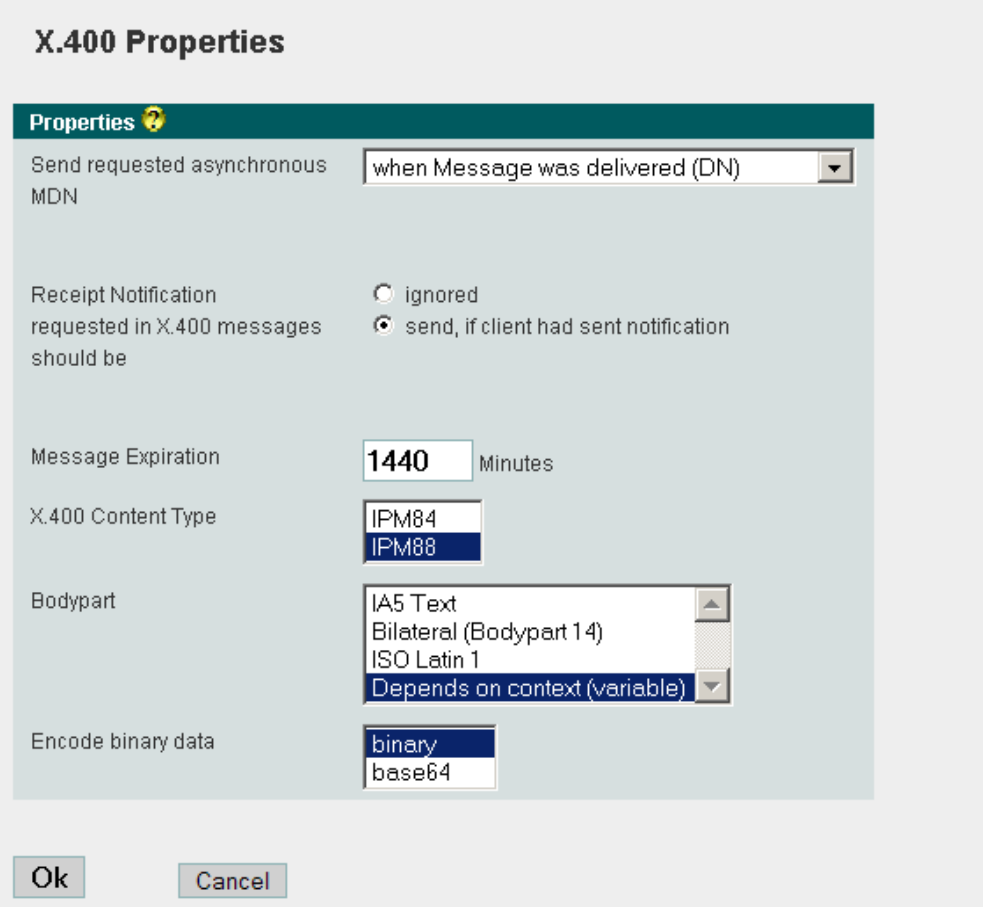
“Inactive“ an AS2 user can temporarily interrupt the delivery of messages and reports (for example when replacing certificates).

If there is a bigger problem or a longer downtime of an user’s application is expected, setting the option “Enable AS2 Bypass” means that all the messages will be moved into the Overrun directory for manual processing.

When the parameter “Duplicate Check” is set the AS2 Gateway will not forward messages to the X.400 partner that an user’s AS2 application has sent twice.

Mapping an AS2 into X.400 message

There are some AS2 specific parameters in the AS2 account properties but most parameters for the mapping between AS2 documents and X.400 messages are equivalent to those of the MessageGate file interface users.



To conform to the AS2 Standard there are four possible values for the menu item "Send requested asynchronous MDN":

- Immediate → Send asynchronous MDN as soon as the message is delivered to the MessageGate process
- When Message has been sent → Send asynchronous MDN if the X.400 message has been sent and the MTA has generated a Message-ID. This Message-ID will set within the MDN (X-MPDUID or MTS-ID).
- When Message has been delivered (DN) → Send asynchronous MDN if the X.400 message has been delivered to the partner's mailbox. This also implies the request for a Non-Delivery Notification!
- When Message has been processed (RN) → Send asynchronous MDN if the message has been processed by the partner's application (read/fetched). This implies the request for a Delivery Notification but a DN is only visible in a status report.

When choosing the value "Immediate" or requesting a synchronous MDN the AS2 user only has the information that the documents were accepted by the AS2 Gateway, but he cannot deduce whether there were problems sending or transferring the X.400 message to the recipient's mailbox. Using the setting "when message was sent" an

AS2 sender only knows that the respective X.400 message has been sent, as he will receive the MTA message identifier X-MPDUID, but he does not know whether the X.400 recipient has received the message or not.

We recommend using the setting “when message was delivered (DN)” (default for this parameter). In such a case the receipt of a positive MDN by the AS2 implies that the message has arrived in the partner’s mailbox. Choosing the setting “when message was processed (RN)“ the AS2 user can receive the information that the partner has processed the message (read/fetched), but the X.400 partner needs to create and send the Receipt Notification in time. Otherwise the AS2 application has to wait too long causing alarms or unnecessary retransmissions.

Using the central EDI functionality

When using the central EDI functionality it is possible to send several X.400 messages while sending a Transmission Set file including the appropriate number of EDIFACT interchanges via AS2. In such a case it is not possible to map the X.400 reports into an asynchronous MDN because each X.400 message may result in the receipt of a report. If the Option “Immediate” is not used the AS2 gateway will send a MDN as soon as the MTA has processed all messages. In the MDN there will be an entry for each EDIFACT interchange ID with the corresponding MTS ID for messages successfully sent or error information (wrong address, syntax error, no EDI relation..) if the message submission failed. If the exact mapping of an X.400 report to a MDN is required then only one EDIFACT interchange should be included in a Transmission Set file.

Example for the text in MDN:

*** IC(s) failed ***

AS2TEST3	0815	:11	NOTEXIST	:65	Receiving Partner not found
AS2TEST4	NOTEXIST	:11	2001005	:65	Sending Partner not found

*** IC(s) submitted ***

AS2TEST1	0815	:11	2001005	:65	X-MPDUID: C8D72CFB11E17CCE85D40FBA
AS2TEST2	0815	:11	2001005	:65	X-MPDUID: C8EDE94B11E17CCE85D413BA

When an X.400 user sends messages to his AS2 partner the “MessageGate” process will send a requested Delivery Notification to the X.400 originator after the message has been transferred to ComAS2. ComAS2 will try to send the document via the AS2 protocol. If the customer’s application is not available ComAS2 will retry transmission dependent on the configured timers (Send timeout, purge time) and increase the interval for every retry as long as there is an entry in the Trace_Tab. The maximum retry interval is 1 hour.

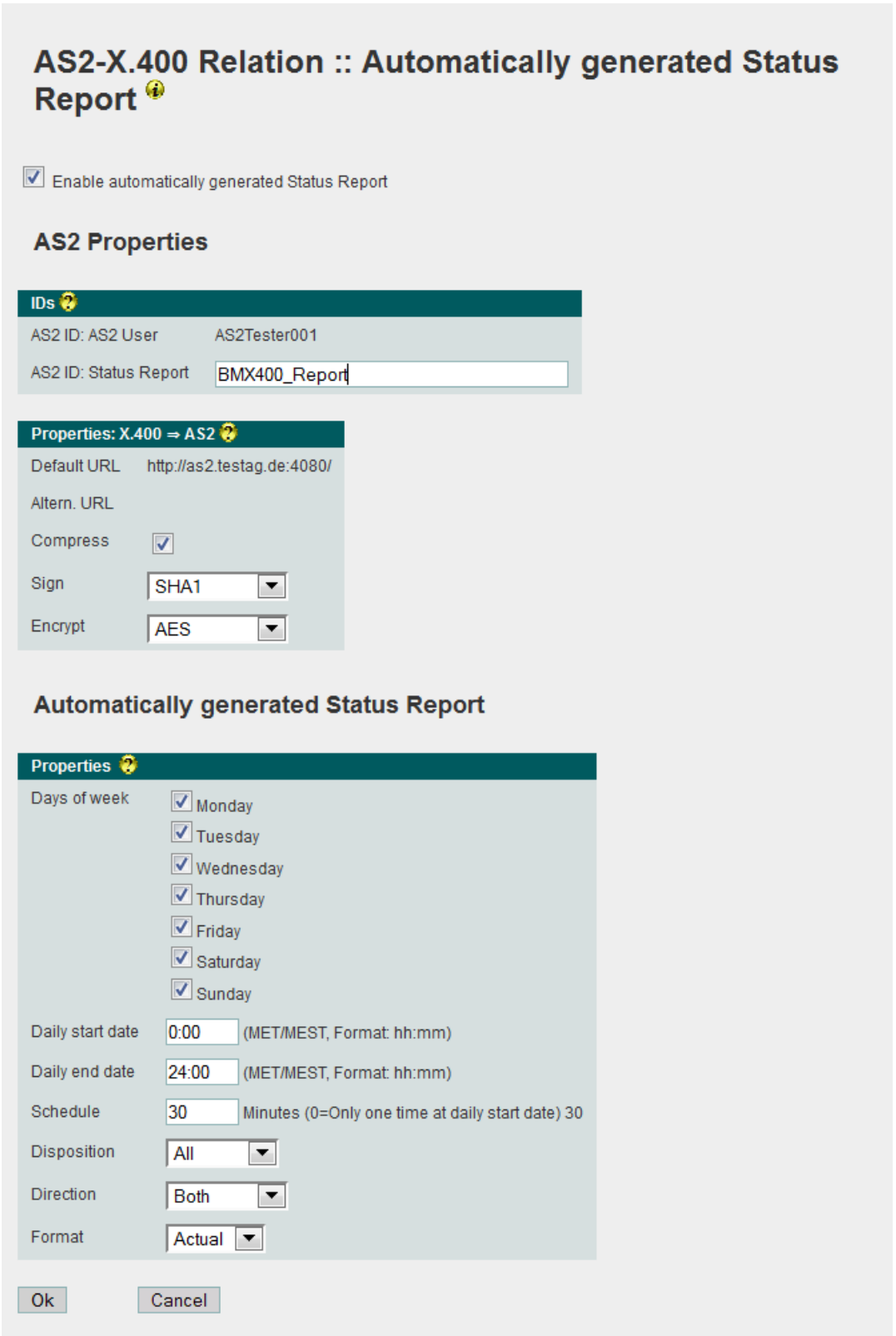
To give X.400 users the possibility to check the delivery of documents to AS2 partner they should request a receipt notification (RN). In the partner profile of the AS2 user the item “Receipt Notifications requested in X.400 messages should be“ should be set to “Send“ so the MessageGate process will create the RN based on the MDN send by Customer’s AS2 application.

Please be aware that the sending of Receipt-Notifications is a chargeable item (added to transfer volume)!

Automatically generated Status Report

As has already been mentioned the AS2 user can use *WebConfig* to request status reports (view or download) or to configure the delivery of status reports via AS2.

To receive status reports via AS2 the AS2 user has to enable this in menu item “Automatically generated Status Report”.



In addition to the options described in Chapter 2.8.8 Configure automatically generated Status Report an AS2 ID had to be assigned for the reporting process and

like all other AS2 trading relations it is possible to define whether compression should be used and the data should be signed or encrypted. If necessary an alternative URL will be configured but a MDN will be not requested.

The first parameters of the status reports entries are equivalent to those of the file interface. However there are some AS2 specific parameters added to these entries to describe the status of AS2 transaction:

Here are the details of those additional parameters:

AS2-ID: AS2 Identifier of X.400 Partner

AS2-MIC: Message Integrity Check identifier sent in Message Header when requesting signed MDN

AS2-Status: Possible values are:

(MDN) not yet send → temporary status of message (Transaction X.400 → AS2) or asynchronous MDN (Transaction AS2 → X.400) which MessageGate transferred to ComAS2

(MDN) still sending → Message (Transaction X.400 → AS2) or asynchronous MDN (Transaction AS2 → X.400) still in ComAS2 retry queue

(async MDN) sent → Message (Transaction X.400 → AS2) or asynchronous MDN (Transaction AS2 → X.400) has been sent

sync MDN sent → synchronous MDN has been sent (Transaction AS2 → X.400)

sync MDN received → Message has been sent (Transaction X.400 → AS2) and synchronous MDN has been received

async MDN requested → Message has been sent (Transaction X.400 → AS2) and asynchronous MDN has been requested

async MDN received → Message has been sent (Transaction X.400 → AS2) and asynchronous MDN has been received

deleted by order → Message (Transaction X.400 → AS2) has been deleted in Overrun directory by user request (in *WebConfig*).

bypassed → Message (Transaction X.400 → AS2) has been moved directly into Overrun directory because „AS2 Bypass“ had been enabled.

send error – bypassed → Message (Transaction X.400 → AS2) has been moved to Overrun directory because send timer had been expired.

send error – discarded → Message (Transaction X.400 → AS2) has been discarded in case of time out (only in Transfermode)

async MDN missing - bypassed → Message (Transaction X.400 → AS2) was sent via AS2 but requested asynchronous MDN did not arrive in time. The message will be moved into Overrun directory. Depending on the setting of the parameter „Retries“ the message transmission may be attempted several times (see also Sentcounter).

async MDN missing - discarded → Message (Transaction X.400 → AS2) was sent via AS2 but requested asynchronous MDN did not arrive in time. The message has been discarded (only in Transfer-

mode). Depending on the setting of the parameter “Retries“ the message transmission may be attempted several times (see also Sentcounter).

send again requested → temporary status when reactivating a message (Transaction X.400 → AS2) transmission that was stored in Overrun directory.

error → temporary status if timer has expired but the message has not been moved yet into the Overrun directory

Message received → AS2 message received but there was no MDN request (Transaction AS2 → X.400)

AS2-Lastsent: Timestamp of the AS2 submission

Format: dd-mmm-yyyy hh-mm-ss +0100 (+0200 MEST)

Sentcounter: Shows how often AS2 Gateway has sent this message (Retries if timer for requested asynchronous MDN has expired)

MDN_expected Date on which the requested asynchronous MDN is expected and has not been received so the data of the transaction will be moved into the Overrun area.
Format: dd-mmm-yyyy hh-mm-ss +0100 (+0200 MEST)

When requesting format „CSV-C“ or „CSV-S“, the CSV file will show the following additional fields (in addition to those already defined in the Chapter):

Field name:	**Explanation:**
AS2-ID	AS2 Identifier of X.400 Partner
AS2-MIC	Message Integrity Check identifier within quotation marks sent in Message Header when requesting signed MDN.
AS2-Status	Possible values see above (within quotation marks)
AS2-Lastsent	Timestamp (UTC/GMT) of the AS2 submission (dd.mm.yyyy hh:mm) (without quotation marks)
Send_counter	Shows how often AS2 Gateway has sent this message (without quotation marks)
MDN_expected	Timestamp (UTC/GMT) the AS2 Gateway expects requested asynchronous MDN (dd.mm.yyyy hh:mm) (without quotation marks)

6 OFTP and MessageGate

6.1 General

The OFTP access users are not aware that they are using MessageGate because the OFTP communication is serviced by a module called ComOFTP (Java communication module produced by Compinia GmbH & Co. KG based on the T-System International GmbH rvsEVO product). The MessageGate process (MGOFTP) accepts OFTP files received via ComOFTP, creates X.400 messages and sends these to the respective partners. X.400 messages destined for an OFTP access user are forwarded directly as files to ComOFTP. ComOFTP transmits these files using OFTP1 (V1.4, TCP/IP) or OFTP2 (V2.0, TCP/IP or TLS) to the configured IP address of the customer's OFTP station (OFTP1 using ISDN and XOT is not supported).

MessageGate also maps X.400 DN (Delivery Notification) and X.400 NDN (Non Delivery Notification) to OFTP EERP (End-to-End Response) / NERP (Negative End Response) respectively and vice versa. Depending on the configured MTA mode the EERP will be mapped to an X.400 Receipt Notification or to an X.400 Delivery Notification.

MTA "Agent"or "Transfer" Mode

If the MTA mode is set to "Agent" (Default), MessageGate will send a requested X.400 DN (Delivery Notification) when the message has been posted to the OFTP communication module (ComOFTP) for transmission to the user's OFTP station. An OFTP EERP or NERP received in response to this transmission will be mapped to an X.400 RN (Receipt Notification) (Read Notification → Status in Report is "Read") or to a Non Receipt Notification (Non Read Notification → Status in Report is "Discarded") if requested by the X.400 partner and enabled by the OFTP access user. If the MTA mode is set to "Agent" the OFTP access user is able to configure the timeout parameter as required by his application.

If the MTA mode is set to "Transfer" an OFTP EERP or NERP sent in response to the message delivery will be mapped to an X.400 DN (status in report is „Delivered") or to an X.400 NDN (Status in Report is "Failed"). A requested X.400 RN will be ignored. When using the MTA "Transfer" mode the X.400/F.400 Standard will determine the message expiry/timeout values (4 hours Urgent, 24 hours Normal and 36 hours Non-Urgent) and an X.400 NDN with the appropriate error code will be sent in response to a message that expires.

Usage of MIME header

To deliver the contents of an X.400 message, that includes several body parts, to an OFTP partner, a MIME structured message with content type „Multipart/mixed" will be used in the file transmitted via OFTP. Similarly, if an OFTP partner wants to send an X.400 message containing several body parts, the OFTP file sent has to be MIME formatted. If the OFTP partner wants to send an X.400 message with only one body part, then it is not necessary for the OFTP file to be MIME formatted (for more details please refer to the next chapter).

Addressing a partner

When using *BusinessMail X.400* OFTP access an OFTP user's X.400 partner always appears as an OFTP partner and similarly an X.400 user's OFTP partner appear as an X.400 partner without any restrictions with regard to the respective transport protocol used.

An OFTP user has different ways to address his X.400 partner. One possibility would be to address the individual Station ID (SID), which is built using the default ODETTE ID of the OFTP access and the User-ID (internal identifier used within *BusinessMail X.400* platform associated with a specific X.400 address*)* of the X.400 partner (O01770000000000X0LUxxxxxx, where the last 6 digits will be replaced by User-ID extended with leading zeros) if this functionality is configured in the relation. The other possibility is to address the X.400 partner using the X.400 partner's User-ID in the first 6 characters of the OFTP VDSN (Virtual Data Set Name = RFC 5024 = SFIDDSN = Virtual File Dataset Name). The rest of the VDSN, separated by a hyphen "-" from the User-ID, will be used for the X.400 Message ID of the X.400 message, which is sent or has been received. When using the individual Station ID the whole VDSN will be used for the X.400 Message ID. The OFTP access will use the values of the parameter "Fixed VDSN" and "Virtual Station" to define whether to use the individual SID or the Standard SID in the header of the file delivered to the customer's OFTP station.

Be aware that for the X.400 Message ID the printable string character set (see Appendix D: characters sets) and for the VDSN the ISO 646 character is used. If there is a problem mapping a character between OFTP and X.400 and vice versa, then this problem character will be a replaced by a hyphen "-" character. The maximum length of an X.400 Message ID is 64 characters, so it is possible that not the complete X.400 Message-ID can be mapped into the VDSN (26 characters). In such a case, only the first 18 characters of the X.400 Message-ID will be used and the last character of the VDSN will be a hyphen "-" character.

We recommend that the X.400 Message ID from the MIME header is used; this can be configured in the OFTP properties of the communication profile. Otherwise the Message ID has to be extracted from the status report. In this case the last character of the VDSN will be a hyphen "-" character. When mapping an incoming OFTP file to an X.400 message, the Message ID from the MIME header will be used, if present and the Message-ID values in the virtual file name will be ignored.

Use of the central EDI function

In WebConfig, for each X.400 partner an OFTP partnership has to be configured, which will display the X.400 partner's User-ID.

There is one exception. OFTP users, as with users of the MessageGate File Interface or the AS2 Gateway, can use the *BusinessMail X.400* central EDI functionality to send EDIFACT documents to X.400 partners or to receive EDIFACT documents. In such a case the OFTP user has to configure an EDI trading relation for each X.400 partner, because the central EDI function will use the header information in the EDIFACT documents to determine the partner's X.400 address.

So when using the central EDI function it is necessary to address the standard Station ID of the OFTP access (ODETTE ID O01770000000000X0LU000000), but it is not necessary to enter the partner's User-ID in the virtual file name, as this will be determined from the Interchange's UNB Header as well as the Message-ID. When using the central EDI function there are no restrictions with regard to the definition of the virtual file name. When files are transmitted to the OFTP partner, as a result of deliver-

ing the EDIFACT content of an X.400 message which has passed the central EDI function, normally (if no “fixed VDSN”) an User-ID of “000000” is used in the VDSN followed by the X.400 Message-ID (which may be truncated, due to the length restriction of the VDSN).

Please be aware of a particular feature of the central EDI function in combination with OFTP access, in comparison to the MessageGate File Interface or EDIBOX (special mailbox type) behavior. Only one EDIFACT interchange per Transmission Set file is supported, because otherwise it would not be possible to map an X.400 report to an EERP/NERP. If a Transmission Set file contains more than one interchange, then only the first interchange will be processed and the other interchanges will be ignored.

When receiving files via OFTP addressing the standard Station ID, ComOFTP will check if the VDSN of each file contains a valid User-ID. If the VDSN does not contain a valid User-ID, ComOFTP checks if the central EDI function is enabled and if the file contains a valid EDIFACT document. The UNB header information is then used to verify the trading relation. If the checks are negative the transmission of an OFTP NERP is initated.

6.2 Differences between File Interface and OFTP Users

The following sections describe an OFTP account configured to run in MTA “Agent” mode where the OFTP user has access to all the *WebConfig* features. This description is also valid for OFTP accounts using the MTA “Transfer” mode, with the exception that the timeout parameters are defined by the X.400 standard as well as certain restrictions with regard to the *Overrun* feature.

For the mapping between OFTP EERP/NERP and X.400 Reports and vice versa the MessageGate process will use the same database relation (Trace_Tab) to store the message status information. An OFTP user can also request a Status Report using the *WebConfig* GUI (View/Download), or configure the delivery of Status Reports via OFTP (for more details about the format of these entries please see the description at the end of this chapter).

The MessageGate process will not delete the database entries once the transaction (data transferred and report sent) is complete. The entries remain in the database until the end of their entry lifetime (determined by the purge time). The *“Purger”* process runs several times a day and deletes the entries that have reached the end of their lifetime (default is 240 hours = 10 days, this can be configured individually on customer request).

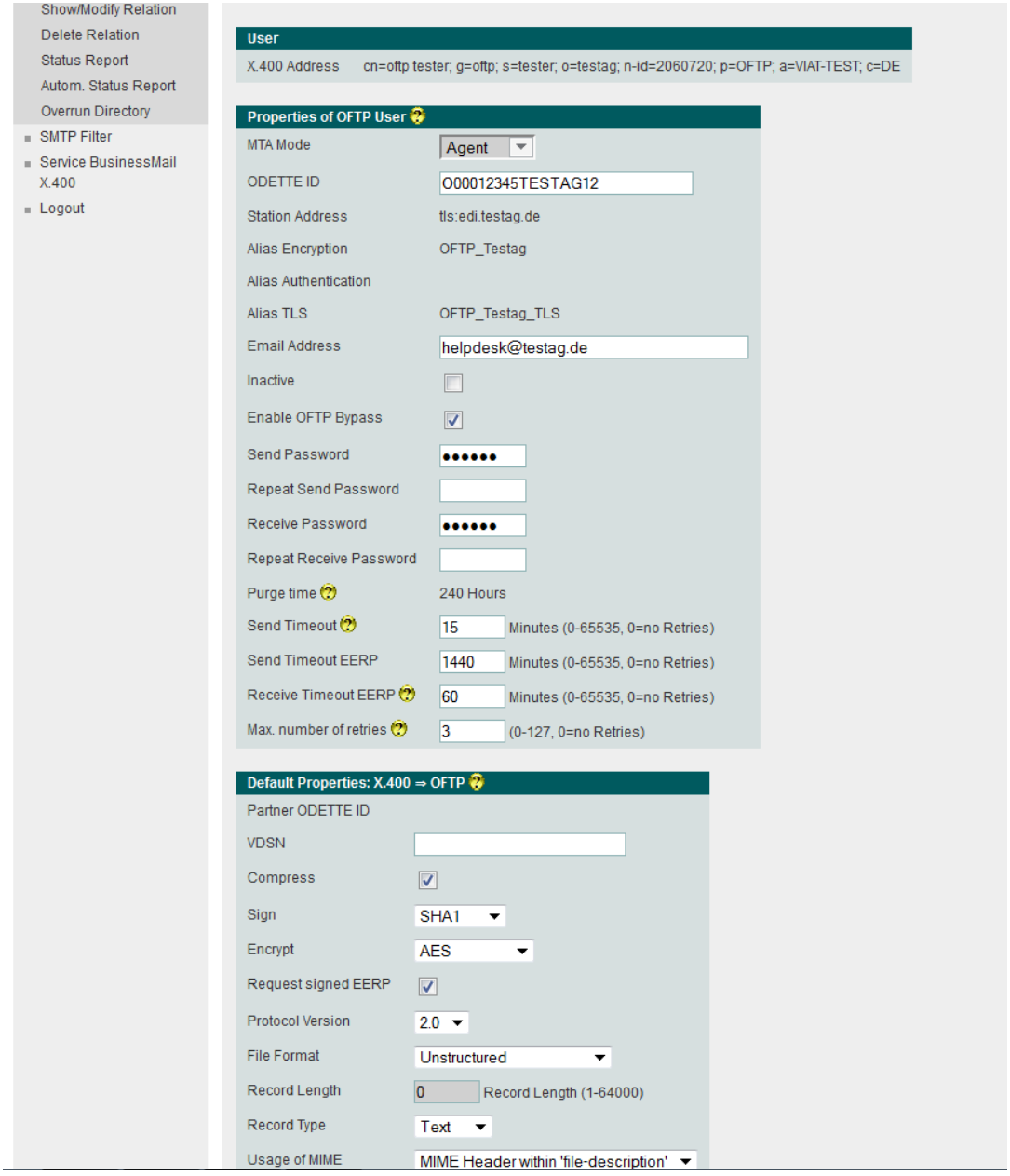
If the *“Purger”* process deletes an entry of a transaction that has not yet completed (for example a requested X.400 RN has not yet been received and ComOFTP has not been able to send an EERP) the final status will be set to “failed”.

An OFTP user is able to request and download Status reports via *WebConfig* and also configure automatically generated Status Report (the sender User-ID “000001” is preconfigured as the prefix). Automatically configured Status Reports (ASR) contain a timestamp instead of the Message-ID in the VDSN next to the prefix.

OFTP Communication Properties

Additional options can be configured for the OFTP Account using *WebConfig* under 'OFTP-X.400 Relation' Properties or Relations. One option is the ODETTE ID (SSID) used by the partner's OFTP station.

The following image shows the first section of OFTP communication properties. The properties of this OFTP account include the MTA Mode configured and the IP address used when sending files (oftps = TLS encrypted, oftp = not encrypted). The type of certificate alias used in conjunction with OFTP2 is also highlighted. If certificate authentication is not configured, it is necessary to configure a send and receive password for the OFTP session authentication. These parameters have to be set accordingly in the partner's OFTP station configuration.



Please be aware, that unlike the AS2 Gateway it is necessary not only to configure one or two certificates in the X.509 Alias, but also all the CA certificates (i.e. the whole chain) have to be stored in the database if self-signed certificates are not used. So the root CA certificate and if present also the intermediate CA certificates have to be imported into the database before a user certificate will be accepted in the X.509 Alias. If the upload of a user certificate fails the CA Upload function in the Menu item X.509 certificate provides the possibility of uploading the accompanying CA certificates.

The purge time (transaction lifetime in the database is set to 240 hours by default) is set by the *BusinessMail X.400* administration, but this value can be configured individually.

When entering a value for the parameter "fixed VDSN" the OFTP access will use this value within the virtual file name (VDSN) of files delivered to the customer's OFTP station. Be aware that there is a dependency on the parameter Virtual station in trading relation. If this parameter is enabled the OFTP access will use the individual Station ID (.O01770000000000X0LUxxxxxx where the last six digits will be replaced with partner's User ID) of this X.400 partner in the file header and will use the value for the virtual file name.

If this parameter is not enabled the OFTP access will ignore the value of the parameter "fixed VDSN" and will use the User-ID and Message ID for the virtual file name.

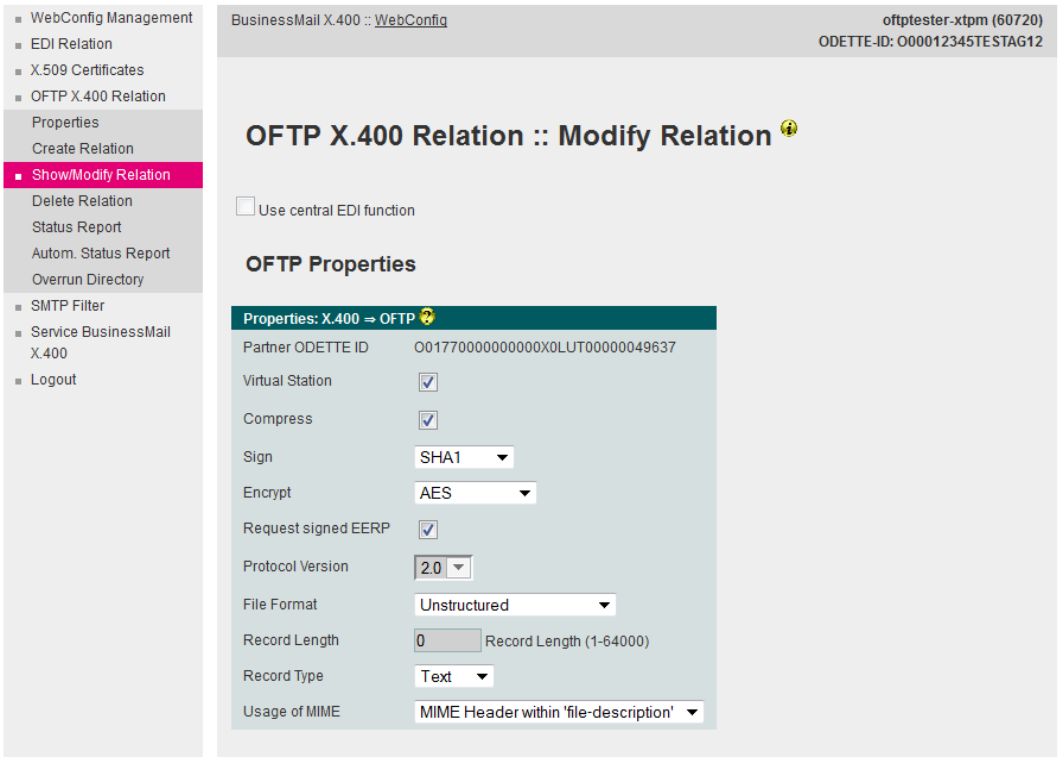
If the parameter is enabled and there is no value set for the parameter "fixed VDSN" the Message ID will be used for the virtual file name.

When using the central EDI functionality the default Station ID, that is the ODETTE ID O01770000000000X0LU000000, will be used and sent in the file header.

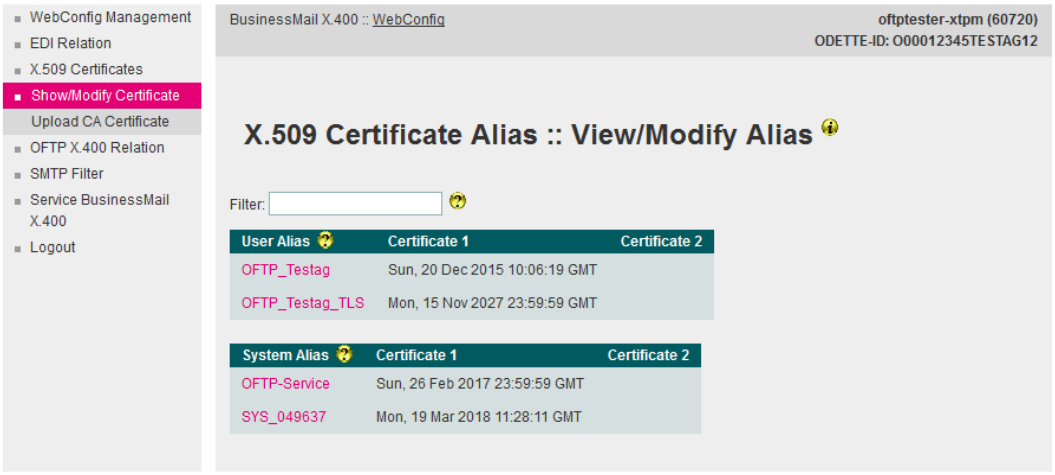
When using OFTP2 it is possible to sign, encrypt and compress files sent to a customer's OFTP station. The signature mechanism (SHA-1, SHA-256, SHA-512) used for the transmission has to be defined in the properties of the OFTP account. In a trading relation there is only the possibility of disabling the signing of files,but not to select another signing mechanism.

Using virtual OFTP station while addressing an X.400 partner

To address an X.400 partner directly via individual station ID and not via an User ID in VDSN a virtual OFTP station has to be configured within the OFTP access where the last 6 digits will show the User ID of the partner (including the leading zero). The menu of the trading relation will show this modified Station ID. Otherwise the default Station ID will be displayed.



In the customer's OFTP station an X.400 partner addressed via an individual Station ID has to be configured as a routed OFTP station. Due to system based restrictions it is not possible to use the certificate/key of the main OFTP station for the virtual stations as well. When configuring a virtual station for an X.400 partner a key and a certificate for this station will be generated automatically. The OFTP user can find and download this certificate needed to encrypt files and verify the signature in the WebConfig menu item X.509 certificates in the section System Alias.

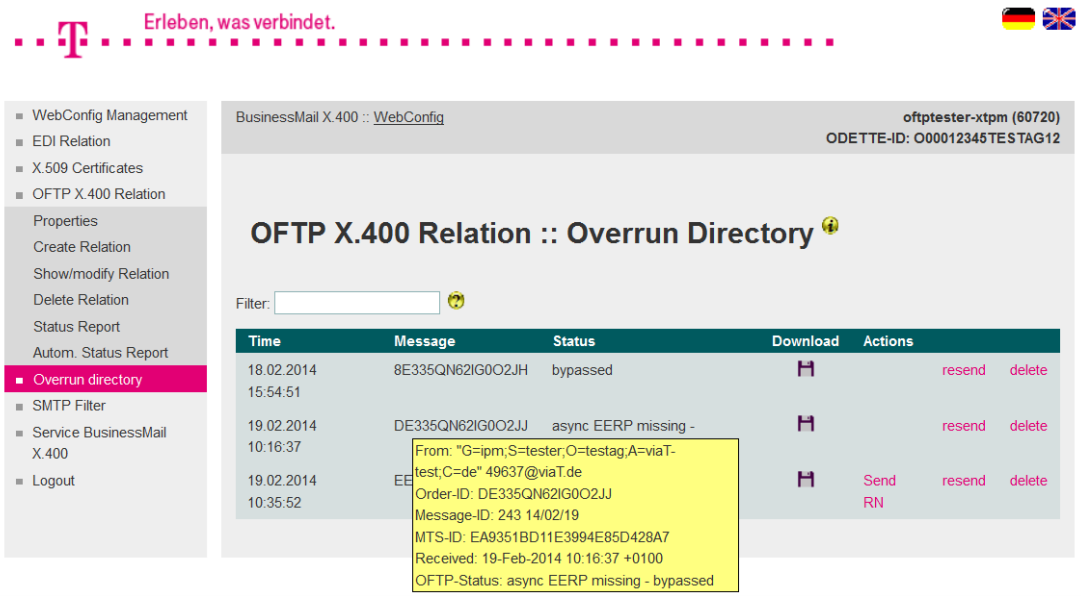


The certificates have a lifetime of 3 years. A few weeks before a certificate is due to expire a new certificate will be generated and displayed in the System Alias section. Information when the OFTP access will replace an existing certificate with a new certificate is also displayed.

OFTP Send Timeout

Apart from the configuration options described above, the customer can define how the OFTP access module should react if problems occur when delivering files or reports to the partner's OFTP station. One can configure how long the OFTP access module should try to deliver a file before moving the data of this transaction into the *Overrun* directory for manual intervention. A user can manage the entries in his *Overrun* directory using *WebConfig* to either download the message user data, to delete the message, or to reactivate the file transmission.

Overrun



The entries in the Overrun directory are available until the "Purger" process deletes these in the database relation (Trace_Tab). If a message stored in the Overrun directory has been reactivated, it will be passed to ComOFTP, even if the parameter *"OFTP Bypass"* is still enabled. The message will only be passed back to the Overrun directory once the Send Timeout timer has expired. Once the requested RN has been transmitted, the transaction is closed and thereafter it is not longer possible to retransmit the message.

When using the MTA "Transfer" mode, it is not possible to send either a DN/NDN or a RN/NRN and the retransmission of a message is limited by the timeout values (message expired) defined in the X.400 protocol.

Send Timeout EERP and retransmission of file

The Send Timeout EERP timeout parameter defines how long the ComOFTP will attempt to deliver an EERP to a partner's OFTP station, before setting the transaction status to "failed".

The two parameters Receive Timeout EERP and Max. number of retries define when the OFTP access module should retransmit a file if the requested EERP has not been received in time and how often the OFTP access module will attempt to retransmit the file. If the parameter Max. number of retries is set to "0" the OFTP access module will move the file directly into the Overrun directory after the *Receive Timeout EERP* timer has expired the first time. If the parameter Max. number of retries value is not "0" the

OFTP access module will attempt to resend the file as often as defined before moving the file into the Overrun directory.

Management of the OFTP Communication in case of a Problem

The parameter Inactive (OFTP Properties) enables a customer to temporarily interrupt the active delivery of files and reports (for example when replacing certificates). However if the partner's OFTP station establishes an OFTP session any queued file for this partner will be sent.

If there is a bigger problem or a longer downtime of the partner's OFTP station is expected, setting the configuration parameter Enable OFTP Bypass means that all the partner's files will be moved into the Overrun directory for manual processing.

Virtual File Format in Properties and Trading Relations

The OFTP WebConfig menus allow for the configuration of:

- the certificate alias (one or two customer certificates) used for:
  - authentication,
  - signature and encryption of files
  - TLS communications in conjunction with OFTP
- the IP address of the partner's OFTP station
  (*oftp:* for TCP connections and *oftps:* for TLS connections)
- default values for sending an X.400 message used within OFTP relation entries (when using OFTP V2.0 whether to compress, encrypt and sign the file or to request a signed response)
- Protocol Version: the supported OFTP version (1.4 for OFTP1 or 2.0 for OFTP2)
- File Format with possible values:
  - "unstructured" (Binary transmission, default),
  - "text" (text content),
  - "fixed record length" (fixed format),
  - "variable record length " (variable format)

  For the File Format selection "fixed record length" and "variable record length " it is possible to set the parameter Record Length to a value between 1 up to 64000 characters and the parameter Record Mode to either "text" or "binary".

Forwarding Additional Message Information

When OFTP2 is used to communicate to a customer's OFTP station it is possible to transmit the subject of a received X.400 message in the OFTP file description field (see RFC 5204 Field SFIDDESC Virtual File Description). The syntax used for this file description field is defined in the WebConfig OFTP properties (X.400=> OFTP) parameter MIME Usage.

This parameter defines, for each relation, how additional message information such as Message-ID or Subject will be transmitted within an OFTP file. A MessageGate process normally uses a MIME header to pass this information. For OFTP the parameter MIME Usage has the following options:

- No MIME header
- Add MIME header to data
- MIME header within 'file description'

When the option "No MIME header" is selected the OFTP access module transmits a file including the user data (pay load) without any additional information. The X.400 messages should contain a maximum of one body part. If the message contains more than one body part a Multipart/MIME content structure without header information will be sent within the payload of the virtual file. When using OFTP2 the subject of the X.400 message will be transmitted in the OFTP2 file description field (without the MIME qualifier "Subject:"). Vice versa if an OFTP2 partner transmits a file with an OFTP V2.0 file description field then this will be mapped to the subject field of the resulting X.400 message. Please be aware that the maximum length of the X.400 subject field is 128 characters and the possible restrictions of the character set (Teletex String). When using this option it is not possible to send X.400 messages that include more than one body part, because the OFTP access module will always copy the contents of the whole file into one body part (the mapping rules applied will be "text" only, "binary" only → BP14, "variable" → based on the OFTP file format). The MIME binary content type is not relevant when not using a MIME header so the corresponding options for the WebConfig parameter Encode binary data (BASE64 or Binary) is not available in the OFTP properties and relations menu.

When the option "Add MIME header to data" is selected, the structure of the virtual file is equivalent to that defined for the MessageGate File Interface. A MIME header is prefixed to the user data that includes message information such as originator- and recipient address, Message-ID, X-MPDUID, Subject and the MIME Content-type.

When sending a message to an X.400 partner and this option has been selected, a MIME header needs to be included, that contains at least the qualifier „Subject: " followed by a blank line preceding the user data. A value for the qualifier "Subject:" is not a prerequisite. Files that address an X.400 partner that do not contain a MIME header will be discarded and a NERP will be sent back to the Originator. In such a case the ComOFTP module will discard the file and there will be no entry in the Trace_Tab for this transaction and it will be not be visible in the Status report. This is equivalent to that case where there is no valid User-ID in the virtual file name and the default Station ID of OFTP access (O017700000000000X0LU000000) was used to address the partner.

If the file contains a corresponding MIME Content-Type: multipart/mixed, it is possible to send an X.400 message with more than one body part. If the MIME header does not contain the Content-Type information qualifier and the WebConfig OFTP properties parameter *Bodypart* is set to "Depends on context (variable)" the OFTP access module determines the X.400 body part type dependent on the OFTP file format type (see Mapping of OFTP file content into X.400 body part).

As has been described above, an OFTP2 partner can send the subject of an X.400 message using the OFTP file description field (using a maximum of 128 of possible 999 characters). However, when the option *"MIME header within 'file description'"* is selected it is necessary to add the qualifier "Subject:" preceding this information, as the file description field can include other MIME qualifiers. If a resulting X.400 mes-

sage is to contain several body parts, the OFTP file description field will contain the MIME structure and the Content-Type qualifier is set to “multipart/mixed”.

The following MIME header field definitions can be found in the OFTP file description field (only with OFTP2) when the OFTP access module delivers (sends) an OFTP file to a partner’s OFTP station:

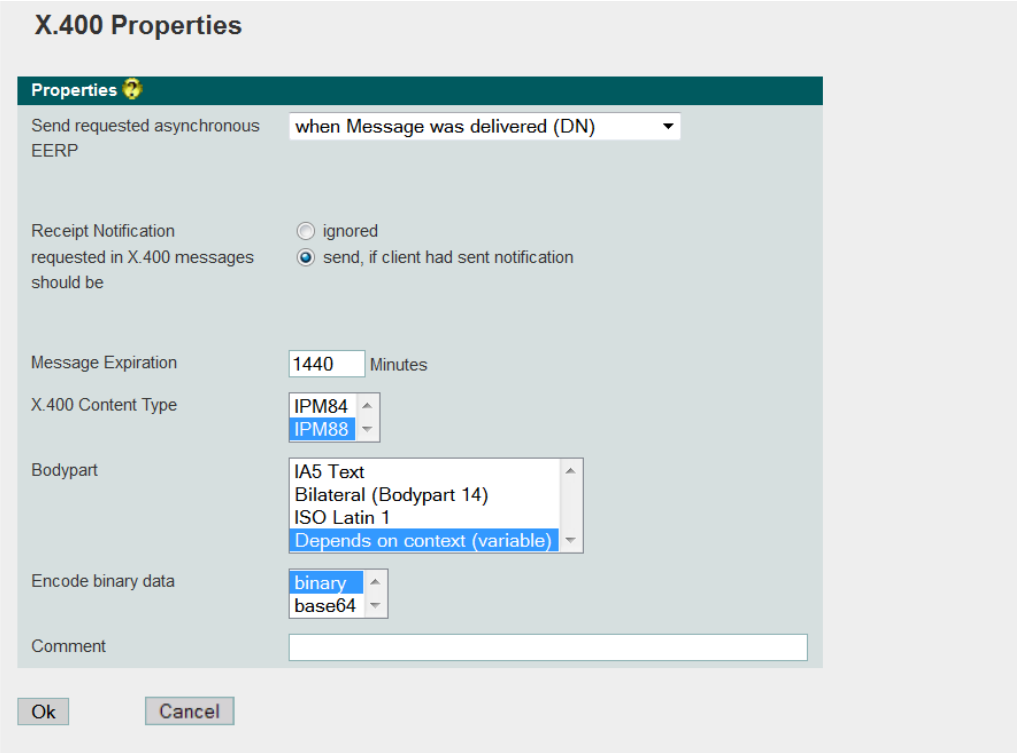
Subject:	(details see, send and receive)
Message-ID:	(details see, send and receive)
X-MPDUID:	(details see, receive only)
Content-Type:	(details see, send and receive)
Content-Disposition:	(details see, send and receive)
Content-Transfer-Encoding:	(details see, send and receive)

Example for the File Description of a file delivered to customer’s OFTP station:

Subject: test MIME Header|Message-Id: 53 14/02/20|X-MPDUID: 31E2D36711E39A4285D45E81|Content-Type: text/plain|Content-Transfer-Encoding: 8bit

Mapping of X.400 Reports into OFTP Responses

In WebConfig there are several configuration options to define the mapping between X.400 reports and OFTP responses in the OFTP X.400 properties and relations.



To conform to the OFTP Standard there are three possible values for the menu item “*Send requested asynchronous EERP*“:

- when Message has been submitted

  → Send EERP if the X.400 message has been sent and the MTA has generated a Message-ID that will be displayed in the status report.

  If submission failed send NERP.
- when Message was delivered (DN)

→ Send EERP if the X.400 message has been delivered to the partner's mailbox.

If the MTA generates a NDN send NERP.

- when Message was read/processed (RN)

  → Send EERP if the message has been processed by the partner's application (read/fetched). This implies the request for a Delivery Notification, but a DN is only visible in a status report.

  If an unprocessed message has been deleted or forwarded send a NERP based on the received NRN.

When choosing the option "when Message has been submitted" an OFTP user is only informed that the respective X.400 message has been sent, but the OFTP user does not know whether the X.400 recipient has received the message or not.

The option "when Message was delivered (DN)" (default for this parameter) is the recommended setting. In such a case the receipt of an EERP by the OFTP user implies that the message has arrived in the X.400 partner's mailbox. Choosing the option "when Message was read/processed (RN)" the OFTP user will receive the information that the partner has processed the message (read/fetched), but it has to be ensured that the X.400 partner (application) creates and sends the Receipt Notification in a timely manner. Otherwise the OFTP application may have to wait too long, which may lead to unnecessary alarms and/or retransmissions.

As already described in a previous section the central EDI function supports only one Interchange per Transmission Set, because otherwise an X.400 report cannot be mapped to an OFTP response.

For messages sent by an X.400 user to an OFTP account using the MTA "Agent" mode the MessageGate process will create a requested delivery notification (DN or NDN) as soon as the message has been passed to the OFTP communication module (ComOFTP). ComOFTP will attempt to deliver the message/file to the partner's OFTP station, dependent on the configured timeout values(send timeout, purge timer). By default, it will attempt to deliver the file as long as there is an entry in the database (ie. the entry has not been purged). Thereafter, the status of the transaction is set to failed.

To give X.400 users the possibility of checking the delivery of documents to OFTP partners, they should request a receipt notification (RN) in their message. In the OFTP partner relation profile X.400 properties the menu item "Receipt Notification requested in X.400 messages should be set to "Send, if client had sent notification" so that the MessageGate process creates the RN based on the EERP sent by the partner's OFTP station.

Please be aware that the sending of Receipt-Notifications is a chargeable item (added to transfer volume)!

For messages sent by an X.400 user to an OFTP partner using the MTA "transfer" mode the MessageGate process will create a requested delivery notification (DN or NDN) as soon as it has received the EERP/NERP (or another OFTP negative transfer response) for the delivered message/ file. The X.400/F.400 standard defines the timeout value during which the attempt is made to send the message/ file (e.g. normal priortity is 24 hours). The Receipt Notification (RN) request in an X.400 message will be ignored in MTA „Transfer" mode.

Mapping of OFTP file content into X.400 Body Part

The parameters configured in the OFTP account properties will be used as the default for new OFTP relations. In each relation it is possible to configure how the content of an OFTP virtual file is mapped into an X.400 message (containing one or more body parts):

- when choosing the value “IA5 Text“
    - the content will always be mapped into a text body part using ASCII (IA5 IRV -> 7 bit) character set (IPM84 and IPM88).
- when choosing the value “ISO Latin 1“
    - the content will always be mapped into a text body part using ISO Latin1 (BP15, General Text, ISO8859-1) character set (IPM84 and IPM88).
- when choosing the value “Bilateral (Bodypart 14)“
    - the content will always be mapped into a binary (BP14, no file info) body part (IPM84 and IPM88).
- when choosing the value “depends on context(variable)“
    - the content will be mapped depending on the OFTP virtual file format or the MIME Content-Type (see below)if present:

OFTP File Format / MIME Content-Type:	**X.400 Body Part**
File Format = text	in BP15/ ISO8859-1 (IPM84 or IPM88)
File Format = unstructured	in BP14 (IPM84 or IPM88)
File Format = fixed record length text	in BP15/ ISO8859-1 (IPM84 or IPM88)
File Format = variable record length text	in BP15/ ISO8859-1 (IPM84 or IPM88)
File Format = fixed record length binary	in BP14 (IPM84 or IPM88)
File Format = variable record length binary	in BP14 (IPM84 or IPM88)
Content-Type = text/plain	in BP15/ ISO8859-1 (IPM84 or IPM88)
Content-Type = applica-tion/EDIFACT	in BP15/ ISO8859-1 (IPM84 or IPM88)
Content-Type = applica-tion/EDI-X12	in BP15/ ISO8859-1 (IPM84 or IPM88)
Content-Type = applica-tion/EDI-content	in BP15/ ISO8859-1 (IPM84 or IPM88)
Content-Type = applica-tion/octet-stream	in BP14 (IPM84 or IPM88)
Content-Type = applica-tion/octet-stream with file	in File Transfer Body Part (FTBP binary

name in content-disposition	body with file info) (IPM88)

Automatically generated Status Report

As described above, an OFTP user like a MessageGate File Interface user can request and download status reports using *WebConfig* or configure the automatic delivery of status reports via OFTP.

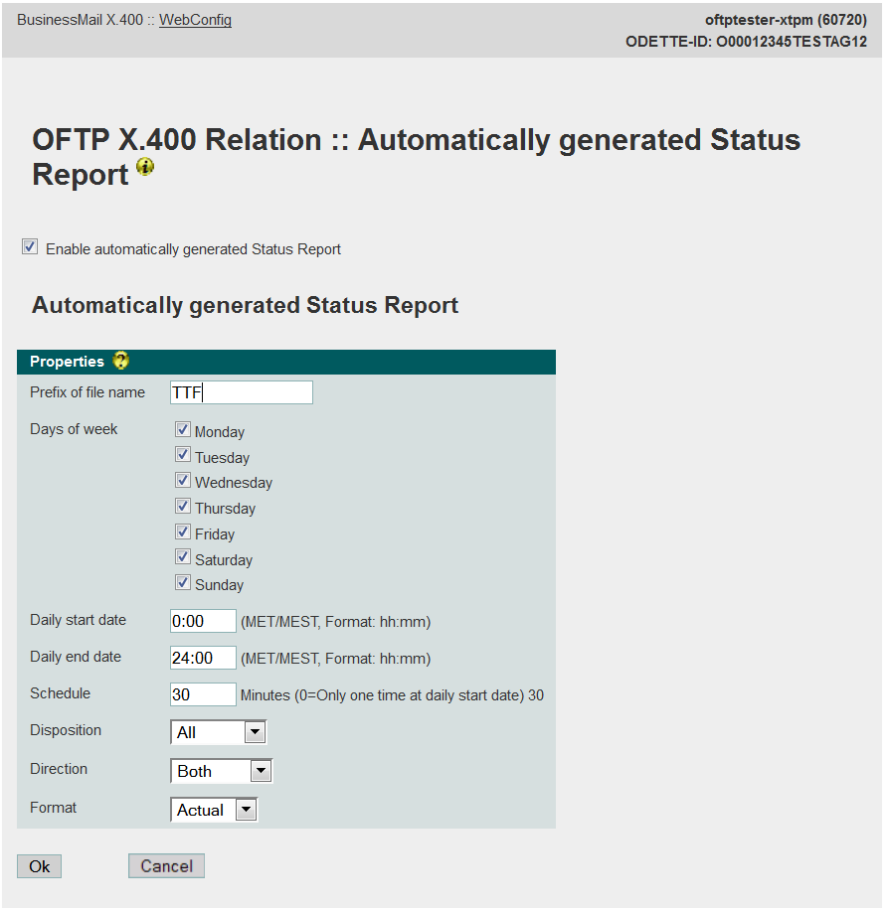
As with the EDI functionality the default Station ID of the OFTP access module (O01770000000000X0LU000000) will be used and as with other OFTP relations it is possible to configure whether the virtual file containing status reports should be compressed, signed and/or encrypted.

Equivalent to the existing File Interface it is possible to configure a prefix. This prefix has by default the value of user id “000001”. This default value can be replaced with a new prefix with a maximum length of 15 characters. The VDSN will contain this prefix followed by a timestamp using the following format *yymmddhhmm*, which differs from the File Interface timestamp format. The prefix and the timestamp will be separated by a hyphen “-“ character.

Example for a VDSN of an automatically generated status report:

000001-1402221204

If there is a value for parameter “fixed VDSN” in the properties of OFTP account it is also possible to use it for the virtual file name of report file. However the prerequisite is that no value is defined for the prefix and/or the preconfigured prefix has been deleted.



The first fields of the OFTP Status Report are equivalent to those for File Interface. However, there are some additional OFTP specific fields, which have been added to these entries to describe the status of an OFTP transaction:

Here are the details of these additional fields:

OFTP status: Possible values are:

- (EERP) not yet sent

  → temporary status of message

  (Transaction X.400 → OFTP) or

  EERP (Transaction OFTP → X.400) which MessageGate transferred to ComOFTP

- (EERP) still sending

  → Message (Transaction X.400 → OFTP) or

  EERP (Transaction OFTP → X.400) still in ComOFTP queue

- (async EERP) sent

  → Message (Transaction X.400 → OFTP) or

  EERP (Transaction OFTP → X.400) has been sent

- async EERP requested

  → Message has been sent (Transaction X.400 → OFTP) and EERP has been requested

- async EERP received

  → Message has been sent (Transaction X.400 → OFTP) and a response has been received. This might be an EERP or a negative response (for example a NERP). The X.400 status shows whether the result of the transaction is positive or negative (using the MTA “Agent“ mode, the status can be “Read:“ or. “Denied:“ and using the MTA “Transfer“ mode the status can be “Delivered:“ or “Failed:“)

- deleted by order

  → Message (Transaction X.400 → OFTP) has been deleted in Overrun directory by user request (in WebConfig)

- bypassed

  → Message (Transaction X.400 → OFTP) has been moved directly to the Overrun directory because „OFTP Bypass“ has been enabled.

- send error – bypassed

  → Message (Transaction X.400 → OFTP) has been moved to the Overrun directory because the send timer has expired

- send error – discarded

  → Message (Transaction X.400 → OFTP) has been discarded because of timeout (only in “Transfer” mode)

- async EERP missing - bypassed

  → Message (Transaction X.400 → OFTP) was sent via OFTP but the requested EERP was not received in time. The message will be moved into the Overrun directory. Depending on the setting of the WebConfig parameter „Retries“ the message trans-

mission may be attempted several times (see also the value of the Sentcounter field).

- async EERP missing - discarded

  → Message (Transaction X.400 → OFTP) was sent via OFTP but the requested EERP was not received in time. The message has been discarded (only in MTA"Transfer" mode). Depending on the setting of the OFTP properties parameter "Retries" the message transmission may be attempted several times (see also Sentcounter).

- send again requested

  → temporary status when reactivating a message /file (Transaction X.400 → OFTP) transmission that was stored in the Overrun directory.

- error

  → temporary status if timer has expired, but the message has not yet been moved into the Overrun directory

OFTP-Lastsent: timestamp of the OFTP submission

Format: dd-mmm-yyyy hh-mm-ss +0100 (+0200 MEST)

Sentcounter: shows how often the OFTP access module has attempted to send this message (Retries if timer for requested EERP has expired)

EERP_expected The lastest date on which the requested EERP was expected but was not received, after which the data of the transaction was moved into the Overrun directory.
Format: dd-mmm-yyyy hh-mm-ss +0100 (+0200 MEST)

When requesting "CSV-C" or "CSV-S" format , the CSV file will show the following additional fields (in addition to those already defined in the Chapter 2.6.4):

Fieldname:	**Description:**
OFTP-Status	Possible values see above (within quotation marks)
OFTP-Lastsent	Timestamp (UTC/GMT) of the OFTP submission (dd.mm.yyyy hh:mm) (without quotation marks)
Sentcounter	Shows how often the OFTP access module has sent this message (without quotation marks)
EERP_expected	Timestamp (UTC/GMT) the OFTP access module expects requested EERP (dd.mm.yyyy hh:mm) (without quotation marks)

7 SMTP MTA and MessageGate

7.1 General

An increasing number of X.400 domain administrators have requested a secure SMTP MTA access to the MailGate X.400 service but do not want to change the X.400 address (Global Domain Identifier ⇨ GDI) of their domain. In order to satisfy this requirement the MailGate X.400 service will now provide a SMTP MTA in addition to existing X.400 MTA.

For this new SMTP MTA a modified MessageGate process will provide the mapping between RFC822 (MIME) and X.400 messages. This new process will connect to the API of a local SMTP MTA and to the API of a local X.400 MTA to allow the message transfer between those two messaging environments.

This new MessageGate process (MGPMDF) will also store transaction logs in a database but the status reports will be only available for the administrators of a customer's E-Mail service and not for the end user of this service. This process will also map RF822 notifications into X.400 reports and vice versa to provide status information to the end users.

The local SMTP MTA is based on the PMDF MTA (Process Software) available on HP OpenVMS.

The current version of the SMTP MTA will not support all mapping rules defined in RFC 2156/2157 (MIXER). Please read the following sections to find out more details about these mapping rules.

7.2 Difference between File Interface and SMTP MTA users

A SMTP MTA user will not connect directly to the MessageGate process because an E-Mail client is used to communicate with his partners. Messages are sent to an appropriate MTA of BusinessMail X.400 using the SMTP protocol. The MessageGate process maps the RFC822 messages into X.400 messages and records each transaction in a database relation (Trace Tab). Reports/Notifications received for sent messages will cause an update of the respective transaction entry. The E-Mail service administrator will see this change when requesting a status report, but the MessageGate process will also send the appropriate SMTP Reports (DSN or MDN) to the originator of the message.

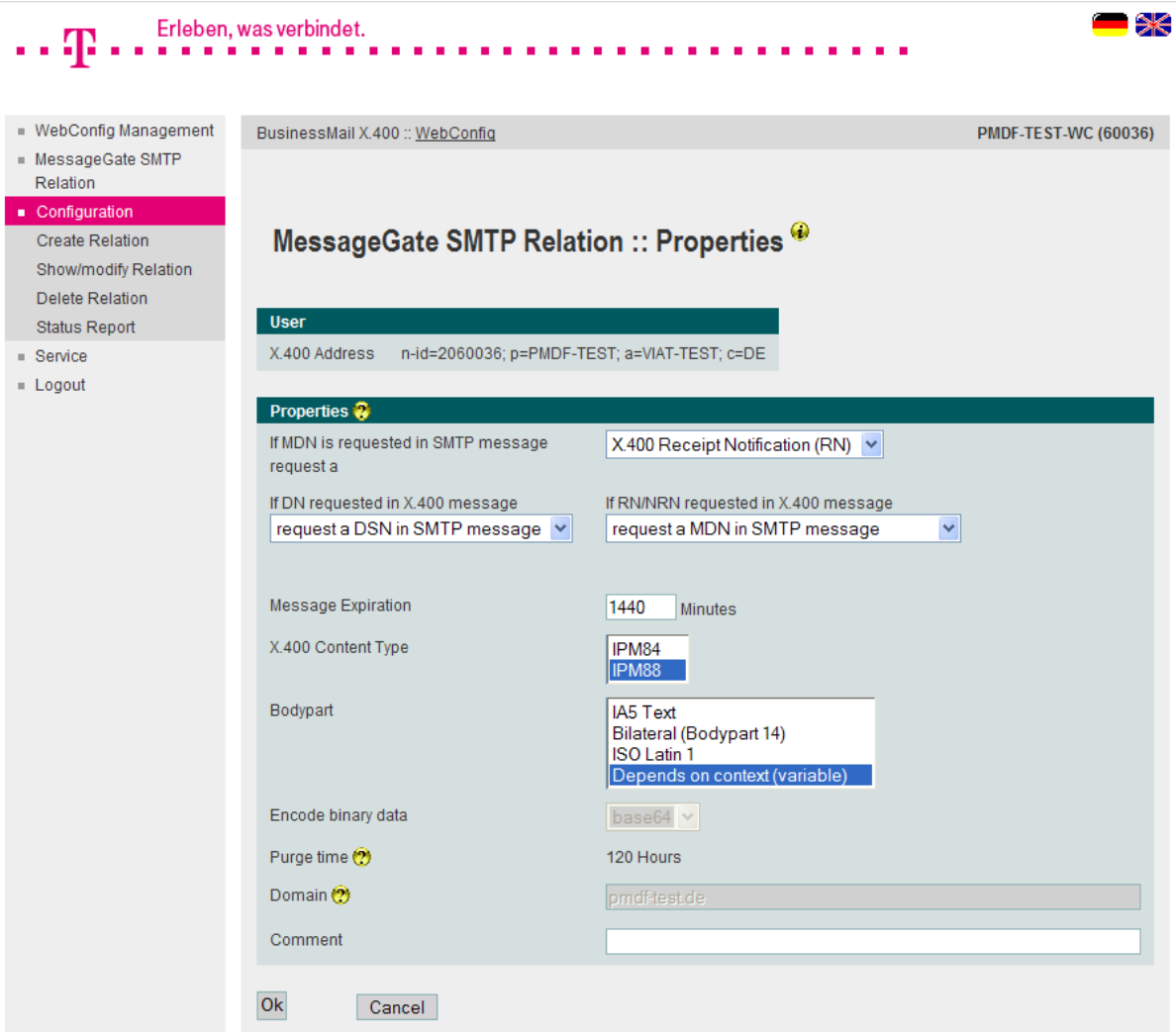
We recommend using an SMTP MTA that supports DSN (Delivery Status Notification, see RFC 1891 or 3461). If this is the case X.400 Delivery Notifications (DN) will be mapped to DSN and X.400 Receipt Notifications (RN) to MDN (Message Disposition Notifications, see RFC 3798) and vice versa.

The MessageGate process also allows you to configure the mapping of X.400 DN requests to MDN requests, but this approach is problematic as this relies on the E-Mail Client/user to create and send an MDN. This cannot be controlled by the administrator of the E-Mail service. The X.400 standard requires that if a delivery notification has been requested that a DN or NDN in the case where a message has not been deliv-

ered is sent within a specified time limit. MGPMDF will send a NDN with reason code „Time expired“ if a MDN is not received in time.

There is also a difference in the behaviour between the File Interface and the SMTP MTA concerning the message content. File Interface users have the choice to define whether binary or BASE 64 format will be used for the binary MIME content. The SMTP MTA only supports BASE64 format for the binary MIME content, but this is the recommended format for RFC822messages.

This is an example of the default properties of an X.400 Domain using SMTP MTA and MGPMDF.



In the menu item “MessageGate SMTP Relation :: Properties” new rules for the mapping of X.400 and SMTP report requests, additional X.400 body part mapping rules and a new option when mapping X.400 into RFC822 address can be found.

The MGPMDF will always map the request for a RFC822 DSN into request for an X.400 DN. MGPMDF will always request an X.400 NDN (Non Delivery Notification), even though no DSN request has been made. So in case of a problem the Email user will receive a DSN with an appropriate error code. For more details see appendix B5. Mapping rules NDN to DSN.

Be aware that the X.400 standard allows the request of different report types for each individual recipient of an X.400 message. It is not possible to map this feature into a SMTP message. So if there is a message sent to different SMTP recipients and in the

X.400 message there is a request for a receipt notification for only some of the recipients the SMTP MTA will not request a MDN.

Partner entries

It is also possible to configure specific partner entries for the domain but the changed properties will be applied to all SMTP MTA users of that particular domain sending mails to this X.400 address. Be aware that the SMTP MTA only uses the mapping rules configured in the partner entries if there is only one recipient per message. If there are more than one recipient in a message the SMTP MTA will use the rules configured in the domain properties.

Address Mapping

In menu item described above you will also find the domain name used for the mapping of RFC822 domain elements to X.400 Oraddress elements. For all the other X.400 address elements MGPMDF will use the mapping rules defined in RFC 2156/2157 (MIXER), where the given name and surname will be added to the Name part of the address field (ie. to the left of the “@“) and the organisation/ organisation-units to the domain part (ie. right of the “@“).

Example: Address mapping (using the domain in the example)

X.400 address: c=de;a=viat-test;p=pmdf-test;o=testag;ou1=entwicklung;s=tester; g=erster

RFC822 address: erster.tester@entwicklung.testag.pmdf-test.de

MGPMDF also offers an extended mapping for migration purposes only, where in addition to the GDI address elements (Country, ADMD, PRMD) the organisation and organisation units will be mapped to to the domain part. So the following mapping roles are also possible:

X.400 address filter: c=de;a=viat-test;p=pmdf-test;o=testag;ou1=entwicklung

Internet mail domain: entwicklung.de

The other X.400 address elements will be added to the left and right hand of the “@“ sign.

So when the SMTP MTA end user receives a message the recipient address will be in the “natural” RFC822 address form.

The format of the originator address and if present, those of the other recipients will be defined in the configuration option “Mapping into SMTP address” available in the properties and partner relation entries.

By default the rule “Use X.400 address syntax“will force the SMTP MTA to place the whole X.400 originator address in the name part of the address field (ie. to the left of the “@“ sign). The X.400 address elements will be separated using the “/“ character. If there is a space or a special character in one of the X.400 address elements the whole X.400 address will be be set between quotation marks (“). Be aware that some of the Email clients will not add the quotation marks when replying to the original message, so the submission of message (refused by own SMTP server) or the delivery (refused by SMTP MTA) will fail.

In such a case please add the quotation marks manually (see also information about Telefax gateway in the following text).

Example for the X.400 address syntax: /G=ipm/S=tester/O=testag/A=viaT/C=de/@ bmx400.de

Alternatively you may use the rule “Mapping of all X.400 address elements” where the SMTP MTA will try to map the X.400 address into a “natural” RFC822 address. If the X.400 address includes elements or characters where there is no counterpart in the “natural” RFC822 address the SMTP MTA will create a “mixed” address. For example there is no mapping for the Commonname or Generation address element and also the “+” character allowed in an X.400 address is not allowed in a “natural” RFC822 address. A space within X.400 address elements will be replaced using tilde sign “~” in RFC822 address.

Example for a “natural“ RFC822 address: ipm.tester@testag.bmx400.de

Example for a RFC822 address with X.400 address elements: /CN=ipm~tester@testag.bmx400.de

The third selection of this option is “Only mapping into natural address”. So if the X.400 originator address or the X.400 address of other recipients contains address elements or characters that does not allow the mapping into a “natural” RFC822 address the SMTP MTA will refuse this X.400 message and create a NDN with the error “conversion not possible” (reason code 2, diagnostic code 8).

When sending messages from SMTP to X.400 it is possible to use a variation of address types. In case of a “natural” or a “mixed” address the SMTP MTA will create an X.400 address based on the rules configured in the database.

A SMTP MTA user can also address other BusinessMail X.400 gateway solutions. When addressing the Telefax gateway it is necessary to set the X.400 address between quotation marks(“) otherwise the “:” character in the X.400 address element “DDA” will cause problems:

Example: “/X121= 0391580217255/DDA:Service=FAX/A=viat/C=de/“@BMX400.DE

A SMTP MTA user may also add an alias to the RFC822 address of an X.400 partner. The SMTP MTA will ignore this alias and also the alias of an originator address when transfering a SMTP message into the X.400 world. The addresses in a delivered SMTP message will not contain an alias.

If the X.400 partner receives a message MGPMDF will have mapped the RFC822 address into an unambiguous X.400 originator address using the rules stored in the profile of the originator’s domain entry. The original originator RFC822 address (the first 64 characters) will be mapped into the X.400 addess element “Freeform name” (Teletex character set), but the the mailbox address will be set into square brackets

Aliasname [givename.surname@domain]

to avoid compatibility problems with older X.400 clients. Microsoft Outlook also uses this kind of address structure within messages.

X.400 Message Structure

RFC 2156/2157 (MIXER) describe the rules to map MIME content type into X.400 body parts. These rules have been implemented in the current version of the SMTP MTA. The MessageGate process now supports the X.400 body part type message.

When choosing the default rule for the option mapping body parts “variable/flat” nested RFC822 message contents (multipart/xxx nested in multipart/mixed) will be mapped without nesting (i.e. flat) into an X.400 message. The MIME contents will be mapped into X.400 body parts depending on their order in the RFC822 message. If the RFC822 message includes a MIME content type multipart/alternate (i.e. the RFC822 message text is present as text as well as an HTML content), the MIME contents will be mapped into appropriate X.400 body parts without any information regarding the identical content.

To map the information about this nested structure into an X.400 message the rule “variable/nested”has to be selected. The nested MIME Content will be mapped into an X.400 message body part where the information about the structure is displayed in the subject field of the message, i.e. alternative message text body parts or HTML documents with imbedded graphics.

In contrast to the File Interface and AS2 the SMTP MTA will accept, in addition to MIME text content with character set ISO-Latin-x (x=1-9) and IA5, also other character sets (i.e. ISO-Latin-15, Windows-1252 or UTF-8). However, if there is no counterpart in X.400 the SMTP MTA will create a BP15 General Text ISO-Latin-1 (ISO 8859-1) body part and adds the MIME header with information about the original character set in front of the text.

Forwarded Messages

In contrast to the File Interface that does not support *forwarded messages,* the SMTP MTA will transfer these in the following manner:

a) An X.400 forwarded message (attachement of type message) to a SMTP MTA user will be stored as a Content-Type message/rfc822 (see RFC 2046). The included X.400 body parts will be imbedded for example in content type multipart/mixed. It is possible to have nested X.400 message imbedded as message/rfc822.

b) There is no standard that defines the structure of a forwarded message within an RFC822 message so MGPMDF will map the header of a forwarded message into a text body (normally the first text body) of an X.400 message and will not map it to a message body part. Only if the forwarded RFC822 message is imbedded as a message/rfc822 content type and the option for mapping body part is “variable/flat” or “variable/nested” will it be mapped into an X.400 message body part. If the rule is set to “IA5-text”, “Bilateral” or “ISO-Latin-1” the MIME structure of a forwarded message will be mapped into an appropriate X.400 body part. The rule “IA5-text” or the option X.400 content type is “IPM84” may cause a loss of information.

Message-ID

When mapping a received X.400 message into a RFC822 message MGPMDF will use the X.400 message id (P2 Message-ID, that the X.400 Client has defined) with a maximum length of 64 characters and will add, seperated by a „#“ character a 16 characters long extension to ensure an unambigous RFC822 message-id. Hence there should be no problem to update the transaction entry when receiving reports generated by SMTP mail services or SMTP mail clients and generate the appropriate X.400 reports.

Spaces within the X.400 message id will be replaced by an underscore (“_“) in the RFC822 message-id. Some RFC822 mail clients have problems with a Message-ID that includes a space character.

Example.: Message-id: <341_11/11/25#EA4A4CI404G0LBPN@tstmt_pmdf.telebox400.de>

When mapping an RFC822 message to an X.400 message MGPMDF uses the first 64 characters of a RFC822 message-id to build the X.400 P2 message-id. The SMTP mail service administrator should ensure that this message-id is unambigious otherwise MGPMDF will not be able to update the transaction entry correctly and to send the appropriate RFC822 notifications.

Status report

In order to facilitate the tracking of transferred messages for SMTP mail service administrators the message entry in the status report will include the originator and the recipient address. The entry will also show the RFC822 message-id (instead of the order id), the X.400 message-id (the message-id of File Interface) and the MTS-id (generated by the X.400 MTA). The other values are equivalent to those of the MessageGate File Interface. So for messages sent from X.400 to SMTP the status report will not show the submission time of the X.400 client but the field „Received:“ will show the time at which MGPMDF has received the message to forward it to the E-Mail recipient. For messages sent from SMTP to X.400 the field „Send:“ will show the time at which MGPMDF had sent the X.400 message.

The status entry for a message sent from SMTP to X.400 will start with “To:“, “Cc:“ or “Bcc:“ and those sent from X.400 to SMTP with a „From:“ address field. The additional recipients will be visible in the message header only. Only in the case where there are several recipients from the same domain will there be an appropriate number of entries in the Trace Tab.

If the RFC822 address includes an alias the address part used for routing will be set in angle brackets (<>). The address will be not set in angle brackets if there is no alias.

Example for a message sent from SMTP to X.400:

To: erster tester </G=erster/S=tester/O=test-ag/A=viaT-test/C=de/@bmx400.DE>
From: test@pmdf-test.de
SMTP-Msg-ID: <4F1D739B.1070307@pmdf-test.de>
X400-Msg-ID: 4F1D739B.1070307
MTS-ID: FE19811D11E145D906005F96
Sent: 23-Jan-2012 15:50:37 +0100
Delivered: 23-Jan-2012 15:50:37 +0100

The RFC822 address will be set in quotes if it includes spaces.

8 Implementation of MessageGate solution

8.1 Using Standard E-Mail Clients

9.1.1 Using Outlook Express

Outlook Express can be used for a first test of the MessageGate functionality to create a message and to send it via MessageGate or to analyze a delivered message and its attachments. Outlook Express provides the capability of storing a message in a text file (Extension *.eml) or to import such a message file.

First configure an E-mail account in Outlook Express and enter the X.400 address in the “Display name” parameter (separate address fields using a semi colon “;” and do not use quotation marks for the address) and for E-Mail address User-ID@viat.de or x@viat.de where User-ID is the local identifier of MessageGate account (e.g. 58111@viat.de). In the fields “Incoming mail server” and “Outgoing mail server” enter “test” because these values will be not used.

Now add a partner address into contacts and enter the X.400 address in last name (separating the x.400 address elements by using semicolons “;” and not using quotation marks for the address) and enter E-Mail address using User-ID@viat.de (e.g. 58111@viat.de) or x@viat.de. For the first test use the address of your own MessageGate account so that you receive your sent test message directly in your own directory.

You are now in a position to create a message and adding configured contacts. Please set the format of the message to plain text. Now add all types of attachments, a selection of characters in the text part of message and a subject. Store the message using “File → send later” into Outbox. Open Outbox, select mail, choose “File → Save as…” and define the name and the path where text file should be stored. Outlook Express will not add a message identifier in a draft message so you should use a file name/order identifier (e.g. M_test00001.eml) that is also usable in an X.400 message identifier. Rename the file to “*.tmp” or upload it directly to the MessageGate directory using FTP or https/WebDAV. When the file transfer is finished rename the file to “*.IN” so that MessageGate processes this file and sends the message. If you have addressed your own account you will find a “M_*.OUT” file in your MessageGate account directory.

You can now download this file, rename it to “*.eml” and open it with Outlook Express. You will see that the message identifier of this mail is the original Order-ID. Outlook Express will be able to handle binary attachments where the content encoding is Base64 or Binary. You can configure the encoding used for a message in the base communication profile or in the partner profile.

9.1.2 Using Mozilla Thunderbird

Using Mozilla Thunderbird it is also possible to create a message for a MessageGate test and to store this in a text file. Thunderbird adds a message identifier when storing a draft message but will not open attachments of imported messages if the content encoding is Binary.

You should first configure a user account and enter User-ID@viat.de (e.g. 58111@viat.de) or x@viat.de in the field E-Mail Address. For the field “Your name:” you should use the X.400 address of your MessageGate account (separate the X.400

address elements using a semicolon ";" and do not use quotation marks for the address). For the field "Incoming server" you may use the string "test" as this value is not used.

You can now add a partner address into the address book by entering the X.400 address (separate the X.400 address elements using a semicolon ";" and do not use quotation marks for the address) in the field "Display" and User-ID@viat.de (e.g. 58111@viat.de) or x@viat.de in the field "E-Mail:". For the first test use the address of your own MessageGate account so that you receive your sent test message directly in your own directory.

now in a position to create a message and adding a configured address. Please set the format of the message to plain text (Options →Format → Plain Text only). Now add all types of other attachments, a selection of characters in the text part of message and a subject. Store the message using "File → send later" into Unsent. Open Unsent, select mail, choose "File → Save as…→ File" and define the name and the path where text file should be stored. Rename the file to "*.tmp" or upload it directly to the MessageGate directory using FTP or https/WebDAV. When the file transfer is finished rename the file to "*.IN" so that MessageGate processes this file and sends the message. If you have addressed your own account you will find a "M_*.OUT" file in your MessageGate account directory.

You can now download this file, rename it to "*.eml" and open it with Thunderbird. You will see that the message identifier of this mail is the original Order-ID. Thunderbird is not able to handle binary attachments where content encoding is Binary. You have to configure that encoding BASE64 will be used when delivering messages in the base communication profile or in the partner profile.

8.2 Designing a MessageGate solution

There are many libraries and tools available to process SMTP/ MIME syntax for a large number of Operating systems and programming languages (both commercial and open source). Hence creating and processing message files should not pose a problem.

Please invest some time in the design of your solution with regard to the handling of unsuccessful transactions. X.400 provides different kinds of reports/notifications for you to implement the tracking of the message transaction status. MessageGate will provide this information in Status Reports.

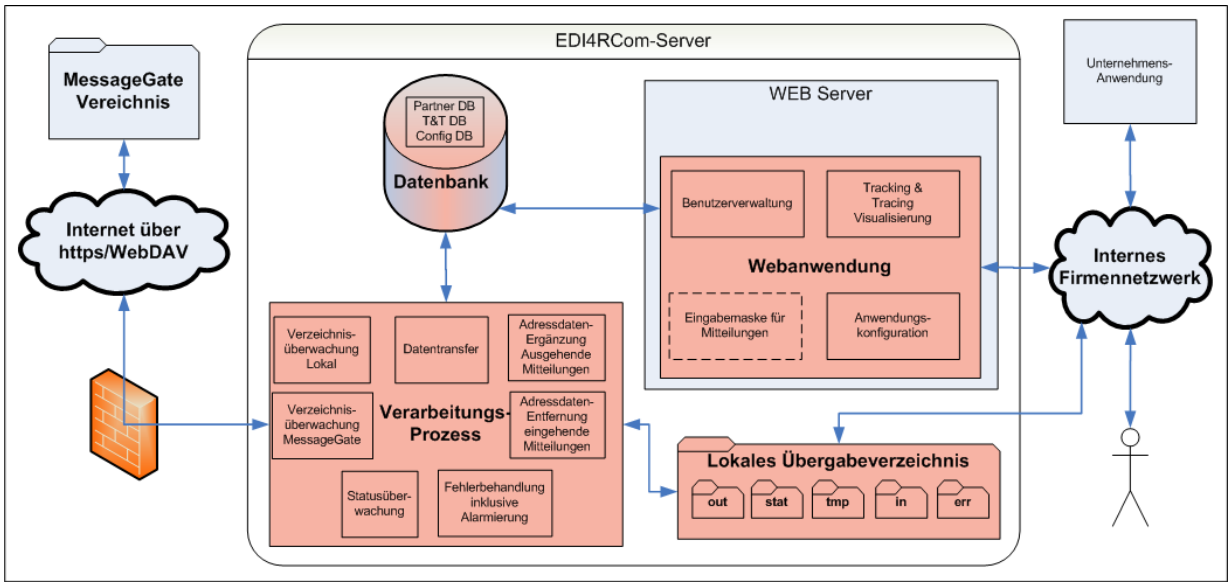
If you do not want to check the delivery of a message you should at least check the Non Delivery or a possible send failure and handle this condition in your application (alarming or resend). If you use the central EDI function we also recommend checking if incoming messages/ EDIFACT documents were refused by the "MessageGate" process. All this information can be found in the Status Reports.

8.3 Open Source Client for MessageGate

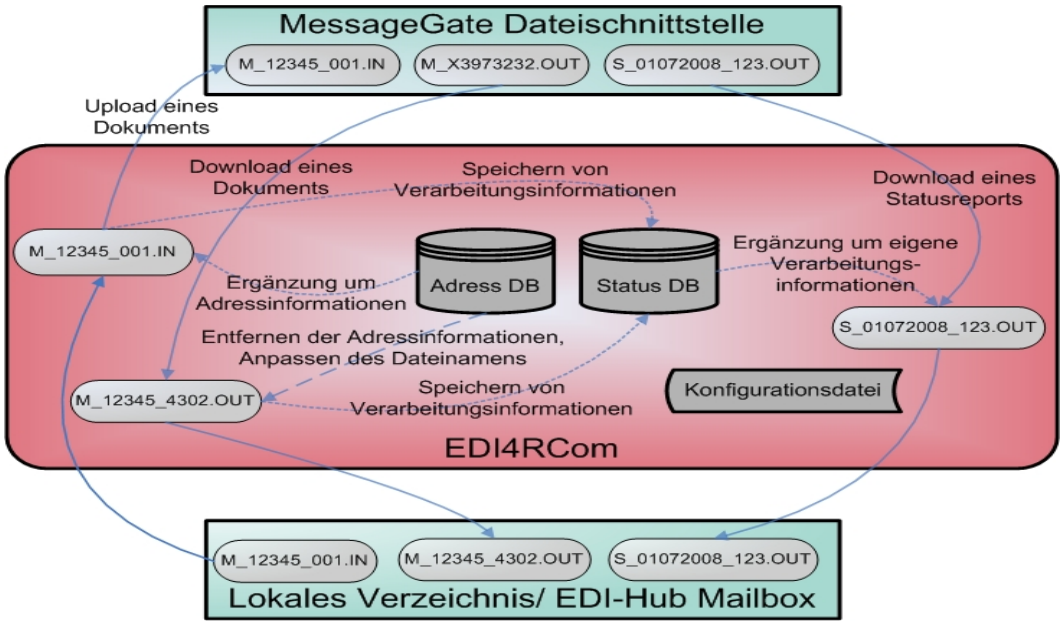
An open source MessageGate client (EDI4RCOM) developed in conjunction with the FH Wiesbaden should provide small and medium companies the possibility of implementing access to MessageGate and the whole X.400 network without a large capital investment for this implementation. The respective client uses Internet and https/WebDAV to send and/or receive messages or EDIFACT documents.

The client was developed using Ruby on Rails and which is supported on most operating systems (Windows 32/64 bit, Linux, UNIX, Max OS etc.). Ruby compared to Java has the advantage that it only allocates memory if the application is started.

The client contains a communication module (on Linux OS this is represented by a daemon; in Windows it has not yet been implemented as a service), a Web based configuration tool (uses the Ruby on Rails integrated Web server module or an already existing server) and an interface to a database (SQLite3 database is included but the client supports other databases, such as MySQL). The client was developed as an extension for the open source library EDI4R that provides implementation framework for EDI applications.

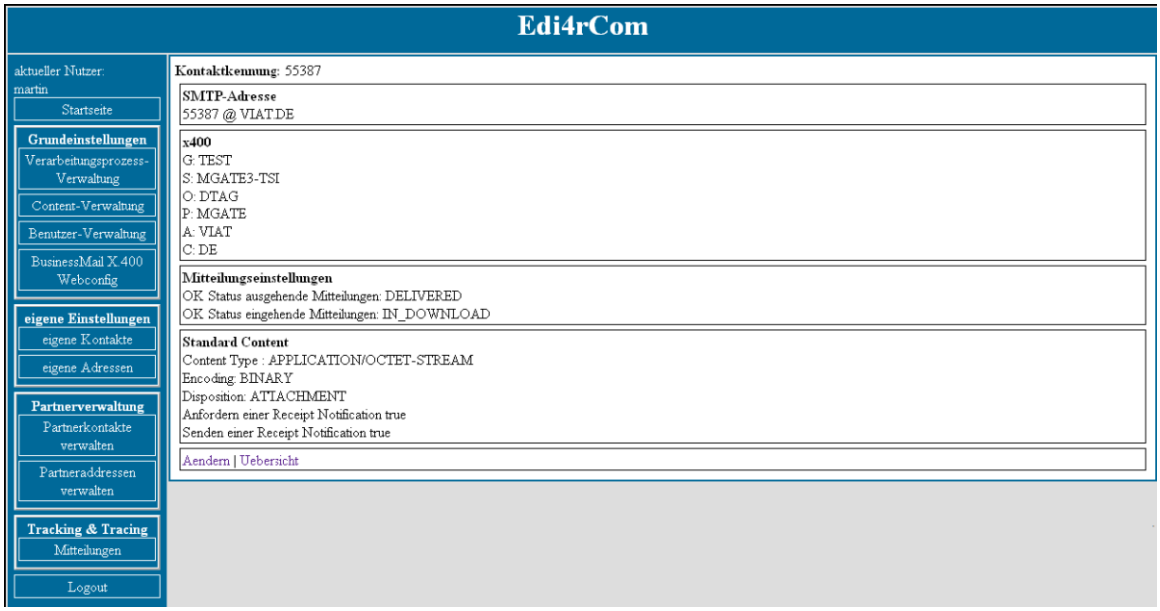


The Web based management tool is able to manage several communication processes which can run on different servers in a customer's network. The communication module frequently checks the MessageGate directory and downloads new messages/data to a local directory. It also checks the local directory to upload messages or EDIFACT documents to the MessageGate directory.

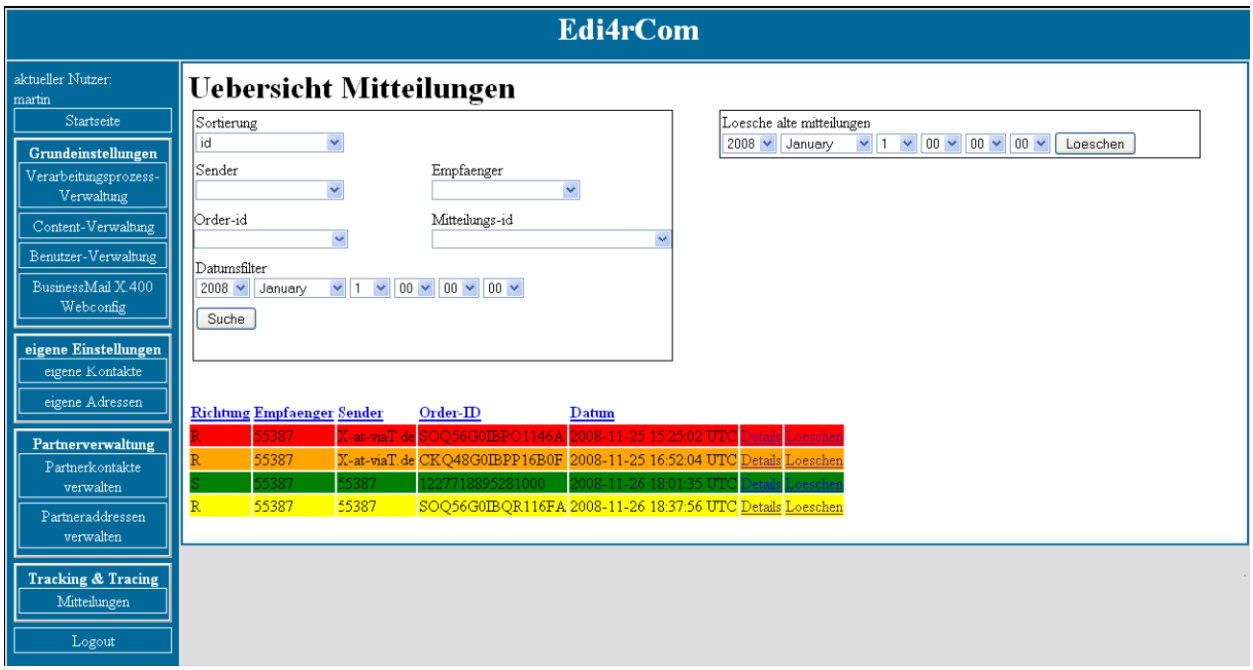


Beside the administration of the communication module

the Web based management tool also provides the administration of contacts and relations (at the present time it is still necessary to manually update entries in *WebConfig*)



and tracking/tracing of transactions to see the status of messages (list of all managed transactions with the option to view the details of each transaction).



The tracking tool stores all requested Status Reports for manual or automatic processing in a local directory.

The program and all the necessary Ruby libraries will be available soon on URL http://www.informatik.fh-wiesbaden.de/~werntges/proj/edi4rcom01.html. Additional information about this client will also be made available soon on the *BusinessMail X.400* service URL http://www.service-viat.de.

The present version of the client does not yet support Multipart/Mixed content so it is only possible to send messages that contain one body part. Downloaded messages with Multipart/Mixed content have to be processed manually. The client will not convert Base64 encoded binary data, so you should configure the properties of your MessageGate account to allow the delivery of 8 bit Binary data.

Appendix A X.400 Address elements

This appendix shows the list of all X.400 Address elements you may use in alias of “To:” and “FROM:” and in host based partner profiles:

C= Country code (3 Characters Printable String)

A= Administrative Domain Name (ADMD, 16 Characters Printable String)

P= Private Domain Name (PRMD, 16 Characters Printable String)

O= Organization (64 Characters Printable or Teletex String)

OU1= Organization Unit 1 (32 Characters Printable or Teletex String)

OU2= Organization Unit 2 (32 Characters Printable or Teletex String)

OU3= Organization Unit 3 (32 Characters Printable or Teletex String)

OU4= Organization Unit 4 (32 Characters Printable or Teletex String)

S= Surname (40 Characters Printable or Teletex String)

G= Given name (16 Characters Printable or Teletex String)

CN= Common name (64 Characters Printable or Teletex String)

N-ID= Box Identifier (UA-ID, 32 Characters Numerical)

X121= Network Identifier (15 Characters Numerical)

T-ID= Terminal Identifier (24 Characters Printable String)

I= Initials (5 Characters Printable String)

Q= Generation (Generation Qualifier, 3 Characters Printable String)

DDA:Type=Value Domain Defined Attributes (Type 8 Characters = Value 128 Characters, both Printable or Teletex String , e.g. dda:service=fax)

See Appendix D for more details about printable string characters.

The following rules

Please remind the following rules for X.400 address:

1. The GDI (Global Domain Identifier), is made up of Country Name, ADMD name and PRMD Name, defines the mail system/mail service. It is necessary to add another address field to define the recipient. This might be Surname, Common name or Unique UA ID.
2. The Unique UA ID might be used as an alternative to a mnemonic address which is made up of name and organizational elements.
3. When using a mnemonic address it might be necessary to define several fields to ensure an unambiguous recipient address
4. An address element Personal Name (PN) which includes Surname, Given name, Initials und Generation Qualifier might be used if the SMTP Gateway sends a message to internet.

Specialties of *BusinessMail X.400* MailBox Service

1. Unlike other X.400 services the *BusinessMail MailBox X.400* service does not require the use of all the address elements when addressing a user of this service. It is sufficient that the recipient address is unambiguous. However the use of such an address carries the inherent risk that it may become ambiguous, if new users are provisioned within the *BusinessMail MailBox X.400* service. In addition an existing trading relation may fail as a result. Hence we recommend the use of the complete X.400 address with all the address elements or to address a user in the *BusinessMail MailBox X.400* service using the User-ID (MessageGate will use the X.400 address configured in the Database) or the Unique Agent ID (Box identifier).

2. When sending messages to a partner in the Internet, who is using a SMTP client, the *BusinessMail X.400* SMTP gateway will be used. When addressing the SMTP gateway the GDI “C=de;A=viat-smtp” needs to be used. To conform to the X.400 standard the surname and if applicable the first name of the SMTP recipient needs to be mapped into the X.400 address element surname. In addition the whole RFC822 address will be mapped into a DDA address element. The type of this DDA element is “RFC-822” and the value is the Internet RFC822 address of the recipient. Please also consider that the “@” is not a valid character in the printable string set so that this needs to be replaced with “(a)”. <x@viat> needs to be added in the following address examples.

For example:

“c=de; a=viat-smtp; g=hans; s=meier; DDA:rfc-822=hans.meier(a)telekom.de”

3. If a fax is sent to your partner then the the *BusinessMail X.400* Fax gateway is used. The GDI of this gateway is “C=de;A=viaT” and the fax number has to be written into the X.400 address element “X121”. The DDA address element where type is “Service“ and the value is “Fax” needs to be added.

For example:

“c=de;a=viaT;X121=061519992725;DDA:service=fax”

For additional information please check http://www.service-viat.de.

Appendix B: Error codes

B1. Error codes of MessageGate Poller process:

Reason code	Error text	Description
0001	Invalid arguments	Internal error. Please contact Helpdesk for further information.
0002	Cannot separate sender ID	Internal error. Please contact Helpdesk for further information.
0003	Invalid file name	Internal error. Please contact Helpdesk or further information.
0004	File-OrderID too long	Order ID is longer than 22 Characters
0005	Cannot open file	File is locked by other process. Please upload file with extension „*.TMP“ first and then rename it to „*.IN“.
0006	Cannot create file	Internal error. Please contact Helpdesk for further information.
0007	Invalid HDR in file	Internal error. Please contact Helpdesk for further information.
0008	Error writing bodypart file	Internal error. Please contact Helpdesk for further information.
0009	Error writing header file	Internal error. Please contact Helpdesk for further information.
0010	Cannot move	Internal error. Please contact Helpdesk for further information.
0011	Wrong parameter specified	File includes invalid values
0012	Empty file	File is empty. Please upload file with extension „*.TMP“ first and then rename it to „*.IN“.
0013	Invalid content in status request file	Request for Status report includes invalid values.
0014	Invalid msg type	Invalid syntax in message structure
0015	Missing header element To:	Mandatory element recipient is missing
0016	Invalid SMTP address	“TO:” or “FROM:” address is invalid (e.g. Alias or RFC822 address part is missing)
0017	Missing header element Content-Type:	Mandatory element definition of data (content) is missing
0018	Missing header element Content-Transfer-Encoding:	Mandatory element definition of transfer encoding content is missing

B2. MessageGate Error codes

Error code	Internal Text symbol	Description
134250499	SHM_EXISTS	shared memory already exists>
134250500	SHM_NOT_EXISTS	shared memory does not exist>
134250501	PRC_DULPNAM	process name %s already exists>
134250505	ATTRIB_INVALID	invalid or unsupported attribute>
134250506	BUFFER_EMPTY	buffer is empty>
134250507	BUFFER_OVERFLOW	buffer overflow>
134250508	BUFFER_TOO_SMALL	buffer too small for primitive>
134250509	NO_BUFFER	no buffer>
134250510	CHECKSUM_INVALID	invalid checksum: %s>
134250511	CLASS_EMPTY	pom_class holds no elements>
134250512	CLASS_END	end of class reached>
134250513	CLASSCTX_NULL	internal error: class context is null>
134250514	CLASSCTX_INVALID	internal error: invalid class context>
134250515	DESCR_NOT_FOUND	descriptor %s not found>
134250516	NO_DEVICE	no device available>
134250517	DIR_CREATE	cannot create directory %s>
134250518	DIR_NAME_INVALID	directory name invalid %s>
134250519	DIR_NOT_FOUND	directory not found %s>
134250520	DIR_NO_ACCESS	no access to directory %s>
134250521	DISK_FULL	disk is full %s>
134250522	DISK_NAME_INVALID	invalid disk name %s>
134250523	DISK_NOT_FOUND	disk not found %s>
134250524	DISK_NO_ACCESS	no access to disk %s>
134250525	DS_INIT	DS API function ds_init failed>
134250526	DS_SHUT	DS API function ds_shut failed>
134250527	DS_BIND	DS API function ds_bind failed>
134250528	DS_UNBIND	DS API function ds_unbind failed>
134250529	DS_ADD_ENTRY	DS API function ds_add_entry failed>
134250530	DS_MODIFY_ENTRY	DS API function ds_modify_entry failed>
134250531	DS_REMOVE_ENTRY	DS API function ds_remove_entry failed>
134250532	DS_SEARCH	DS API function ds_search failed>
134250533	ELEM_LENGTH_MISS	tried pom_write on an element created without length>
134250534	ELEM_NOT_FOUND	cannot find element of specified type %s>
134250535	ELEM_READONLY	tried to modify readonly element %s>
134250536	ELEM_NOT_PRESENT	element not present>
134250537	ELEM_MULTI_VALUED	element is multi-valued>
134250538	ENCOD_ANY	ANY syntax found in %s>
134250539	ENCOD_END	end of encoding; %s>
134250540	ENCOD_EXCEEDED	encoding exceeds 4 bytes length>
134250541	ENCOD_INVALID	invalid encoding; %s>
134250542	ENCOD_EOC_EXPECTED	expected EOC; %s>
134250543	ENCOD_INCOMPLETE	incompleted decode; %s>
134250544	ENCOD_LENGTH	element length exceeded; %s>

134250545	ENCOD_EMPTY	tried to encode an empty primitive; %s>
134250546	ENCOD_MANDATORY	missing mandatory element; %s>
134250547	ENCOD_LIMIT	limit exceeded; %s>
134250548	UNSUP_EXTID	ExtensionId %s is not supported>
134250549	ENTITY_ACCESS	invalid access method for entity>
134250550	ENTITY_ATTR	invalid type %s of entity attribute>
134250551	ENTITY_TYPE	invalid entity type>
134250552	ENTITY_SLOT_INV	invalid slot number %s for entity>
134250553	ENTITY_SLOT_NOFR	no slot free for entity>
134250554	ENTITY_TYPE_ATTR	expected attribute TYPE>
134250555	ENTITY_CMD_NOTSUPP	command not supported>
134250556	ENTITY_RESTART	can not restart entity %s>
134250557	ENTITY_ATTR_TAB	attribute description not found>
134250558	ENTITY_DUPLNAM	name for entity already exists>
134250559	ENTITY_MGMT	Master not active>
134250560	ENTITY_NOT_EXIST	entity not exist>
134250561	ENTITY_WILDCARD	wildcard not supported>
134250562	ENTITY_CREATE	can not create entity %s>
134250563	ENTITY_LIMIT	Entity %s exceeds restarting limit>
134250564	MGMT_SHUTDOWN	OMS system is down>
134250565	ENTITY_NORESTART	restarting not allowed>
134250566	ENTITY_ABNORMAL	Entity %s terminated abnormally>
134250567	ENTITY_ERROR	Entity %s terminated due to an error>
134250568	ENTRY_NOT_FOUND	found no or no more entry>
134250569	ENTRY_IGNORE	ignore this entry>
134250570	ENTRY_EXISTS	entry already exists>
134250571	ENTRY_ISCHILD	cannot delete child-entry without its parent>
134250572	ENTRY_SELECT	entry selected by MSK>
134250573	ENV_LOG	environment/logical %s not set>
134250574	EXPR_EMPTY	%s-expression is empty>
134250575	FEAT_NOT_SUPP_YET	feature not supported yet>
134250576	FILE_CONNECT	cannot connect to record access block of file %s>
134250577	FILE_CREATE	cannot create file %s>
134250578	FILE_DELETE	cannot delete file %s>
134250579	FILE_END	end of file detected %s>
134250580	FILE_BEGIN	beginning of file detected %s>
134250581	FILE_FREE	cannot release lock (possibly not set), file: %s>
134250582	FILE_LENGTH	attempt to read past end of file %s>
134250583	FILE_LOCK	cannot lock file %s>
134250584	FILE_NAME_INVALID	invalid filename %s>
134250585	FILE_NO_SUCH	no such file: %s>
134250586	FILE_OPEN	cannot open file %s>
134250587	FILE_READ	error reading on file %s>
134250588	FILE_SEEK	cannot seek to file position, file: %s>
134250589	FILE_TRUNCATE	cannot truncate file %s>
134250590	FILE_WRITE	error writing to file %s>

134250591	FILE_PARTIAL	cannot read as many bytes as asked for>
134250592	FUNC_NOT_IMPLEM	function %s not implemented>
134250593	FUNC_SDS_NOT_EXIST	this function will never exist>
134250594	FUNC_SEQUENCE	invalid sequence of function-calls>
134250595	IPC_KEY	invalid key name %s>
134250596	IPC_LOCK_NOT_GRANT	lock not granted>
134250597	IPC_MBX_REMOVED	message queue is removed>
134250598	IPC_CREATION	process creation error (%s)>
134250599	IPC_MBX	message queue error (%s)>
134250600	IPC_LOCK	locking error (%s)>
134250601	IPC_SHM	shared memory error (%s)>
134250602	IPC_LNM	logical name error (%s)>
134250603	IPC_NO_LOGTAB	logical name table %s for mailbox does not exist>
134250604	IPC_NO_PRIV	insufficient privilege for IPC operation>
134250605	IPC_USRQUOTA	quota of user %s failed (%s)>
134250606	IPC_USER_UNKNOWN	user %s unknown>
134250607	IPC_LOGNAM	error on logical name passed through VMS function>
134250608	LOCSUBM_VIOLATED	non local submission>
134250609	MATCH_INAPPR	inappropriate matching>
134250610	MEMORY_INSUFF	no memory>
134250611	MODE_LOCK_UNKNOWN	unknown locking mode %s>
134250612	MODE_OPER_UNKNOWN	got unknown operation mode %s>
134250613	MSG_CONTENT_LONG	content too long>
134250614	MSG_CONTENT_MULTI	more than one content>
134250615	MSG_CONTENT_NONE	content missing>
134250616	MSG_ENV_MISS	envelope missing>
134250617	MSG_ENV_WHAT	unknown element in envelope>
134250618	MSG_IFC_NONE	child entry without IFC entry encountered>
134250619	MSG_MISSING	message missing>
134250620	MSG_NOT_REC	no message received>
134250621	MSG_NOT_SEND	no message sent>
134250622	MSG_ORIGIN_MULTI	more than one originator>
134250623	MSG_ORIGIN_NONE	originator missing>
134250624	MSG_ORR_MULTI	more than one originator report requested>
134250625	MSG_ORR_NONE	no originator report requested>
134250626	MSG_RECIP_NONE	recipient missing>
134250627	MSG_RECNAME_MULTI	more than one recipient name>
134250628	MSG_RECNAME_NONE	no recipient name>
134250629	MSG_REPORT_WHAT	unknown element in report>
134250630	MSG_ORIGIN_INVALID	invalid message originator>
134250631	MTA_CANCEL	MTA function ma_cancel failed,%s>
134250632	MTA_CLOSE	MTA function ma_close failed,%s>
134250633	MTA_FINISH_DEL	MTA function ma_finish_delivery failed,%s>
134250634	MTA_NOT_AVAIL	MTA not available>
134250635	MTA_NO_MPDU	MTA has not MPDU %s>

134250636	MTA_OPEN	MTA function ma_open failed,%s>
134250637	MTA_START_DEL	MTA function ma_start delivery failed,%s>
134250638	MTA_SUBMIT	MTA function ma_submit failed,%s>
134250639	MTA_WAIT	MTA function ma_wait failed,%s>
134250640	MTA_AGENTNAME	MTA agent name invalid>
134250641	OCOM_PORT_INVALID	Invalid port number>
134250642	OCOM_FREE	The osak has queued the request. There is free block>
134250643	OCOM_QUEUED	The osak has queued the request>
134250644	OCOM_DISRUPTED	A disruptive event has occured>
134250645	OCOM_INVAEI	The application entity invocation is invalid>
134250646	OCOM_INVDEFCTXT	The default context response is invalid>
134250647	OCOM_INVFUNC	The call is invalid>
134250648	OCOM_INVFUS	The functional units are invalid>
134250649	OCOM_INVID	The activity identifier is too long>
134250650	OCOM_INVPCTXT	The presentation context list is invalid>
134250651	OCOM_INVSYNCPNT	The synchronization point serial number is invalid>
134250652	OCOM_NOPROCINFO	The is no process-id and no process-name>
134250653	OCOM_NOSYNCPNT	The synchronization point serial number is missing>
134250654	OCOM_TRANSERR	There is error in transport provider>
134250655	OCOM_NOEVENT	There is no event>
134250656	OCOM_INCPCI	The PCI is not complete>
134250657	OCOM_INSFWS	There is not enough workspace in the parameter block>
134250658	OCOM_NOBUFFERS	There are not enough user data buffers>
134250659	OCOM_OVERFLOW	Too much user data has been sent for session v-1>
134250660	OCOM_INVTOKEN	The token setting is invalid>
134250661	OCOM_INVEVENT	There is invalid event>
134250662	OM_CREATE	Object Management function om_create failed,%s>
134250663	OM_DELETE	Object Management function om_delete failed,%s>
134250664	OM_GET	Object Management function om_get failed,%s>
134250665	OM_INSTANCE	Object Management function om_instance failed,%s>
134250666	OM_PUT	Object Management function om_put failed,%s>
134250667	OM_READ	Object Management function om_read failed,%s>
134250668	OM_WRITE	Object Management function om_write failed,%s>
134250669	OPER_UNKNOWN	Operation %s is unknown>

134250670	PARAM_INVALID	invalid parameter %s>
134250671	PARAM_NULL	parameter %s was a NULL pointer>
134250672	LENGTH_INVALID	invalid length %s>
134250673	PORT_INVALID	invalid port %s>
134250674	PRIV_MISSES	process misses privilege>
134250675	PVERS_INVALID	protocol version invalid>
134250676	QUEUE_EMPTY	empty queue>
134250677	QUOTA_EXHAUSTED	process quota exhausted>
134250678	RANGE_REVERSED	range reversed>
134250679	RANGE_NOTVALID	range out of bounds>
134250680	RESTR_EXCEEDED	restrictions exceeded>
134250681	RULE_UNKNOWN	rule %s is unknown>
134250682	SERVER_BUSY	server is busy>
134250683	SERVER_DOWN	server is down>
134250684	SIGNAL_NOT_SUPP	Signal (interrupt) is not supported: %s>
134250685	SQL_ERROR	SQL error: %s>
134250686	STATE_INVALID	current facility state does not allow this operation>
134250687	STATUS_NEW_DEL	tried to delete a NEW-message>
134250688	STATUS_CHANGE	change from actual status to given is not supported>
134250689	STATUS_UNKNOWN	status %s is not known>
134250690	STRUCT_USER_ERROR	got wrong structures from user agent>
134250691	SYNTAX_DIFFERENT	different OM_syntax between pom_add and pom_write>
134250692	SYNTAX_UNKNOWN	given OM_syntax %s is unknown>
134250693	SYNTAX_ERROR	syntax error>
134250694	TABLE_FULL	table overflow>
134250695	TABLE_UNKNOWN	tried to lock an unknown MDB-table %s>
134250696	TAG_TOO_BIG	tag too big .gt. 4 bytes>
134250697	TRANSACTION_INACTIVE	Transaction %s inactive>
134250698	TRANSACTION_ACTIVE	Transaction %s active>
134250699	TRANSACTIONID_WRONG	Transaction Id %s wrong>
134250700	TYPE_DIFFERENT	different OM_type between pom_add and pom_write>
134250701	USER_AMBIGUOUS	user name is ambiguous>
134250702	USER_NEW_NOT_SPEC	existing user name has same elements plus some other>
134250703	USER_OLD_NOT_SPEC	existing user name has same elements but fewer>
134250704	USER_PWD_INVALID	invalid password given by user>
134250705	USER_UNKNOWN	user name is unknown>
134250706	USER_DOUBLE_LOGIN	user is already logged in %s>
134250707	USER_ACTIV_NOT_DEL	cannot delete user with status ACTIVE>
134250708	USER_NAME_NOT_MOD	orname elements modify only single user>
134250709	USER_PWD_EXPIRED	user password expired>
134250710	USER_SRVC_EXPIRED	user service expired>

134250711	USER_EDI_DENIED	no agreement between EDI sender and receiver>
134250712	USER_EDI_NO_SND	Sending Partner not found>
134250713	USER_EDI_NO_REC	Receiving Partner not found>
134250714	USER_EDI_NO_AGROP	Agreement for open receiver not found>
134250715	USER_EDI_NO_AGRCL	Agreement for closed receiver not found>
134250716	USER_MAX_LOGIN_FAILS	maximum login fails reached>
134250717	DOMAIN_AMBIGUOUS	domain name is ambiguous>
134250718	ORNAME_INVALID	no valid addressing form specified>
134250719	USER_EDI_NO_RUT	Routing Partner not found> !
134250720	USER_DISCONN_NOT_DEL	cannot delete user with status DIS-CONNECTED>
134250721	VERSION_INVALID	version invalid>
134250722	VALUE_TOO_BIG	value too long>
134250723	WRONG_VALUE	wrong values: %s>
134250724	WRONG_VALUE_TYPE	value type is unknown: %s>
134250725	WRONG_VALUE_LENGTH	value length is incorrect>
134250726	WRONG_VALUE_NUMBER	digits in value is not a number>
134250727	WRONG_VALUE_MAKEUP	make-up of value is wrong>
134250728	WRONG_VALUE_RANGE	value out of range>
134250729	WRONG_VALUE_SYNTAX	wrong value syntax>
134250730	WILDCARD_INVALID	wildcard not allowed>
134250731	DECODE_END	end of decoding>
134250732	NO_SUCH_SND	no such sender>
134250733	NO_SUCH_REC	no such recipient>
134250734	TP_AMBIGUOUS	trading partner is ambiguous>
134250735	NO_SUCH_RUT	no such router>
134250736	NO_DEFAULT_VALIDFOR	no default validfor-entry available>
134250737	HAVE_SPECIAL_VALIDFOR	special validfor-entries still exist>
134250738	LOGONNAME_AMBIGUOUS	logonname is ambiguous>
134250739	MANDATORY_ATTRIBUTE	mandatory attribute missing>
134250740	MANDATORY_SECTION	mandatory section missing>
134250741	MANDATORY_TABLE	mandatory table missing>
134250742	BCKP_PURG	Backup/Purger/Repair cannot run parallel>
134250743	TIME_RELATIVE	cannot convert relative time into UTC format>
134250744	CFG_TOKEN_UNKNOWN	found unknown token in config file>
134250745	CFG_TOKEN_AMBIGUOUS	found ambiguous token in config file>
134250746	CFG_SYNTAX	found token without '=' in config file>
134250747	CFG_VALUE_UNKNOWN	value not found in conversion table>
134250748	CFG_VALUE_AMBIGUOUS	value has ambiguous conversion>
134250749	CFG_VALUE_SYNTAX	syntax error in config file>
134250750	CFG_VALUE_NOTMULTI	config value is not multi valued>
134250751	CFG_TABLE_SYNTAX	error in conversion table>
134250752	EDPRS_INVIC	invalid interchange syntax>
134250753	EDPRS_INVTRAIL	invalid interchange trailer>
134250754	EDPRS_INVHEAD	invalid interchange header>
134250755	EDPRS_RUBBISH	too many useless characters>

134250756	EDPRS_CTRLREF	control reference mismatch>
134250757	EDPRS_TAGLONG	found too long EDI tag>
134250758	EDPRS_ELEMLONG	found too long EDI element>
134250759	EDPRS_TOOMANYIC	too many Interchanges>
134250760	PARSE_BREAK	break current parsing>
134250761	UTL_LOCK_CREATE	Lock create failed>
134250762	UTL_LOCK_DESTROY	Lock destroy failed>
134250763	UTL_LOCK	Locking failed>
134250764	UTL_UNLOCK	Unlocking failed>
134250765	POMSORT_IGNORED	pom type %s ignored (reflist: %s)>
134250766	STOP_RESOURCE	out of resources>
134250767	ADDINFO	Additional info: %s>
134250768	RSC_NOT_FOUND	Resource information not found>
Under certain circumstances you will see the error code of another host process instead of that of MessageGate (see the following example). Please send this error code to the Helpdesk to analyze this problem.		
159416462		MTA function ma_submit failed,%s

B3. MTA Error codes (Non Delivery Notification)

Error codes in NDN:

Reason code	X.400 Standard	Description
0	Transfer-failure	Indicates that, while the MTS was attempting to deliver or probe delivery of the subject-message, some communication failure prevented it from doing so.
1	Unable-to-transfer	Indicates that, due to some problem with the subject itself, the MTS could not deliver or probe delivery of the subject-message.
2	Conversion-not-performed	Indicates that a conversion necessary for the delivery of the subject-message could not (or cannot) be performed.
3	Physical-rendition-not-performed	Indicates that the PDAU was unable to physically render the subject-message.
4	Physical-delivery-not-performed	Indicates that the PDS was unable to physically deliver the subject-message.
5	Restricted-delivery	Indicates that the recipient subscribes to the restricted-delivery element-of-service (as defined in Recommendation X.400) which prevented (or would prevent) the delivery of the subject-message.
6	Directory-operation-unsuccessful	Indicates that the outcome of a required directory operation was unsuccessful.
7	deferred-delivery-not-performed	Indicates that a request for deferred delivery of the subject-message was unable to be performed;
8	transfer-failure-for-security-reason	Indicates that, while the MTS was attempting to deliver or probe delivery of the subject-message, a security failure prevented it from doing so

Reason codes in NDN

Diagnostic Code	X.400 Standard	Description
0	Unrecognized-OR-name	The recipient-name argument of the subject does not contain an OR-name recognized by the MTS.
1	Ambiguous-OR-name	The recipient-name argument of the subject identifies more than one potential recipient (i.e., is ambiguous).
2	MTS-congestion	The subject could not be progressed, due to congestion in the MTS
3	Loop-detected	The subject was detected looping within the MTS.
4	Recipient-unavailable	The recipient MTS-user was (or would be) unavailable to take delivery of the subject-message.
5	Maximum-time-expired	The maximum time for delivering the subject- message, or performing the subject-probe, expired.
6	Encoded-Information-Types-unsupported	The encoded-information-types of the subject-message are unsupported by the recipient MTS-user.
7	Content-too-long	The content-length of the subject-message is too long for the recipient MTS-user to take delivery (exceeds the deliverable-maximum- content-length).
8	Conversion-impractical	A conversion required for the subject-message to be delivered is impractical.
9	Implicit-conversion-prohibited	A conversion required for the subject-message to be delivered has been prohibited by the originator of the subject.
10	Implicit-conversion-not-subscribed	A conversion required for the subject-message to be delivered has not been subscribed to by the recipient.
11	Invalid-arguments	One or more arguments in the subject were detected as being invalid.

12	Content-Syntax-error	A syntax error was detected in the content of the subject-message (not applicable to subject-probes).
13	Size-constraint-violation	Indicates that the value of one or more parameter(s) of the subject violated the size constraints defined in the X.411 Recommendation, and that the MTS was not prepared to handle the specified value(s).
14	Protocol-violation	Indicates that one or more mandatory argument(s) were missing from the subject.
15	Content-type-not-supported	Indicates that processing of a content-type not supported by the MTS was required to deliver the subject-message.
16	Too-many-recipients	Indicates that the MTS was unable to deliver the subject-message due to the number of specified recipients of the subject-message.
17	No-bilateral-agreement	Indicates that delivery of the subject-message required a bilateral agreement where no such agreement exists.
18	Unsupported-critical-function	Indicates that a critical function required for the transfer or delivery of the subject- message was not supported by the originating-MTA of the report.
19	Conversion-with-loss-prohibited	A conversion required for the subject-message to be delivered would have resulted in loss of information; conversion with loss of information was prohibited by the originator of the subject.
20	Line-too-long	A conversion required for the subject message to be delivered would have resulted in loss of information because the original line length was too long.
21	Page-split	A conversion required for the subject-message to be delivered would have resulted in loss of information because an original page would be split.

22	Pictorial-symbol-loss	A conversion required for the subject-message to be delivered would have resulted in loss of information because of a loss of one or more pictorial symbols.
23	Punctuation-symbol-loss	A conversion required for the subject-message to be delivered would have resulted in loss of information because of a loss of one or more punctuation symbols.
24	Alphabetic-character-loss	A conversion required for the subject-message to be delivered would have resulted in loss of information because of a loss of one or more alphabetic characters.
25	Multiple-information-loss	A conversion required for the subject-message to be delivered would have resulted in multiple loss of information.
26	Recipient-reassignment-prohibited	Indicates that the MTS was unable to deliver the subject-message because the originator of the subject prohibited redirection to a recipient - assigned-alternate-recipient.
27	Redirection-loop-prohibited	The subject-message could not be redirected to an alternate-recipient because that recipient had previously redirected the message (redirection-loop).
28	Dl-expansion-prohibited	Indicates that the MTS was unable to deliver the subject-message because the originator of the subject prohibited the expansion of DLs.
29	No-dl-submit-permission	The originator of the subject (or the DL of which this DL is a member, in the case of nested DLS) does not have permission to submit messages to this DL.
30	Dl-expansion-failure	Indicates that the MTS was unable to complete the expansion of a DL.
31	Physical-rendition-attributes-not-supported	The PDAU does not support the physical-rendition-attributes requested.

32	Undeliverable-mail-physical-delivery-address-incorrect	The subject-message was undeliverable because the specified recipient postal-OR-address was incorrect.
33	Undeliverable-mail-physical-delivery-office-incorrect-or-invalid	The subject-message was undeliverable because the physical-delivery-office identified by the specified recipient postal-OR address was incorrect or invalid (does not exit).
34	Undeliverable-mail-physical-delivery-address-incomplete	The subject-message was undeliverable because the specified recipient postal-OR-address was incompletely specified.
35	Undeliverable-mail-recipient-unknown	The subject-message was undeliverable because the recipient specified in the recipient postal-OR-address was not known at that address.
36	Undeliverable-mail-recipient-deceased	The subject-message was undeliverable because the recipient specified in the recipient postal-OR-address is deceased.
37	Undeliverable-mail-organisation-expired	The subject-message was undeliverable because the recipient organization specified in the recipient postal-OR-address has expired.
38	Undeliverable-mail-recipient-refused-to-accept	The subject-message was undeliverable because the recipient specified in the recipient postal-OR-address refused to accept it.
39	Undeliverable-mail-recipient-did-not-claim	The subject-message was undeliverable because the recipient specified in the recipient postal-OR-address did not collect the mail.
40	Undeliverable-mail-recipient-changed-address-permanently	The subject-message was undeliverable because the recipient specified in the recipient postal-OR-address has changed address permanently (Tmoved'), and forwarding was not applicable.

41	Undeliverable-mail-recipient-changed-address-temporarily	The subject-message was undeliverable because the recipient specified in the recipient postal-OR-address has changed address temporarily (T on travel'), and forwarding was not applicable.
42	Undeliverable-mail-recipient-changed-temporary-address	The subject-message was undeliverable because the recipient specified in the recipient postal-OR-address had changed temporary address (Tdeparted'), and forwarding was not applicable.
43	Undeliverable-mail-new-address-unknown	The subject-message was undeliverable because the recipient has moved and the recipient's new address is unknown.
44	Undeliverable-mail-recipient-did-not-want-forwarding	The subject-message was undeliverable because delivery would have required physical-forwarding which the recipient did not want.
45	Undeliverable-mail-originator-prohibited-forwarding	The physical forwarding required for the subject-message to be delivered has been prohibited by the originator of the subject-message.
46	Secure-messaging-error	The subject could not be progressed because it would violate the security-policy in force.
47	Unable-to-downgrade	The subject could not be transferred because it could not be downgraded (see Annex B to Recommendation X.419).
48	Unable-to-complete-transfer	Delivery failed (e.g. size of message exceeds limit)
49	Transfer-attempts-limit-reached	Maximum number of attempts to establish a connection for message transfer reached
50	Incorrect-notification-type	The report type defined in message is not corresponding to content of message
51	Dl-expansion-prohibited-by-security-policy	The subject-message was addressed to a Distribution List, but the security policy prohibited expansion of that DL
52	Forbidden-alternate-recipient	The subject-message would have been redirected, but the new recipient is unacceptable for security reasons

53	Security-policy-violation	The security-policy is violated
54	Security-services-refusal	The security services requested cannot be supported
55	Unauthorised-dl-member	The DL-expansion was not performed because the MTA discovered that one of the members of the Distribution List was prohibited by the security policy from receiving this message
56	Unauthorised-dl-name	The MTA has detected that the recipient OR-name identifies a Distribution List but the local security policy does not permit the onward transfer towards the DL-expansion point
57	Unauthorised-originally-intended-recipient-name	The OR-name of the originally intended recipient of the redirected or DL-expanded message is unauthorised for security reasons
58	Unauthorised-originator-name	The originator MTS-user OR-name is unauthorised for security reasons
59	Unauthorised-recipient-name	The recipient MTS-user OR-name is unauthorised for security reasons
60	Unreliable-system	Delivery of the subject-message would require that the subject-message be transferred to an insecure system, which is incompatible with the message security label
61	Authentication-failure-on-subject-message	Validation of the content-integrity-check, message-originauthentication-check, or message-token (i.e. signature, or any other token data) argument of the subject-message failed, and therefore the contents of the subject-message could not be authenticated or validated
62	Decryption-failed	The subject-message content could not be decrypted
63	Decryption-key-unobtainable	The required key could not be obtained to decrypt the message-token encrypted-data or for content confidentiality

64	Double-envelope-creation-failure	The security policy required the creation of an outer envelope to protect the subject-message. However, the MTA was unable to create the outer envelope
65	Double-enveloping-message-restoring-failure	The subject-message contained an inner envelope, but failure of security services on the outer envelope prevented the MTA from extracting the inner message for subsequent processing
66	Failure-of-proof-of-message	A fault was detected in the proof-of security arguments in the subject-message;
67	Integrity-failure-on-subject-message	Validation of the content-integrity-check argument of the subject-message failed, and therefore the contents of the subject-message could not be validated
68	Invalid-security-label	The security policy identifier in the message security label identifies a policy which is known to the recipient UA or MTA, but which is not acceptable to that system
69	Key-failure	The required keys could not be obtained
70	Mandatory-parameter-absence	A mandated security element for compliance with the security-policy in force is absent
71	Operation-security-failure	The transfer or delivery operation failed for security reasons
72	Repudiation-failure-of-message	The security policy required use of a signature with non-repudiation properties, but the subject-message was not signed with a non-repudiable signature on origination
73	Security-context-failure	The message security label is incompatible with the security-context in force
74	Token-decryption-failed	The message token could not decrypted
75	Token-error	An error has been detected with the message-token argument of the subject-message

76	Unknown-security-label	The security policy identifier in the message security label is not recognised by the recipient UA or MTA. Such a policy is not supported by that system
77	Unsupported-algorithm-identifier	The recipient does not support the algorithm identifiers used in the security argument of the subject-message
78	Unsupported-security-policy	The recipient does not support the required security-policy, as identified in the message-security-label argument of subject-message

B4. X.400 User Agent Error codes (Non Receipt Notification)

Error codes in NRN:

Code number	X.400 Standard	Description
0	IPM-discarded	Message was discarded
1	IPM-auto-forwarded	Message was auto forwarded and there is no guarantee for the processing of this message

Reason to discard messages:

Code number	X.400 Standard	Description
0	IPM-expired	Message has expired
1	IPM-obsoleted	Message is not valid
2	User-subscription-terminated	User agreement is not longer valid

B5. Mapping rules NDN to DSN

X.400 Reason code	X.400 Diagnostic Code	X.400 Standard	SMTP Action
6	0	Unrecognized-OR-name	5.1.1
6	1	Ambiguous-OR-name	5.1.4
0	2	MTS-congestion	5.4.5
0	3	Loop-detected	5.4.6.
0	4	Recipient-unavailable	5.2.1
0	5	Maximum-time-expired	5.4.7
2	6	Encoded-Information-Types-unsupported	5.6.1
1	7	Content-too-long	5.3.4
2	8	Conversion-impractical	5.6.3
2	9	Implicit-conversion-prohibited	5.6.2
2	10	Implicit-conversion-not-subscribed	5.6.5
1	11	Invalid-arguments	5.5.4
1	12	Content-Syntax-error	5.5.2
1	13	Size-constraint-violation	5.5.0
1	14	Protocol-violation	5.5.0
1	15	Content-type-not-supported	5.6.1
1	16	Too-many-recipients	5.5.3
1	17	No-bilateral-agreement	5.7.1
1	18	Unsupported-critical-function	5.5.1
2	19	Conversion-with-loss-prohibited	5.6.5
2	20	Line-too-long	5.6.5
2	21	Page-split	5.6.5
2	22	Pictorial-symbol-loss	5.6.5
2	23	Punctuation-symbol-loss	5.6.5
2	24	Alphabetic-character-loss	5.6.5
2	25	Multiple-information-loss	5.6.5
1	26	Recipient-reassignment-prohibited	5.4.0
1	27	Redirection-loop-prohibited	5.4.0
1	28	Dl-expansion-prohibited	5.7.2
1	29	No-dl-submit-permission	5.7.2
1	30	Dl-expansion-failure	5.2.4
3	31	Physical-rendition-attributes-not-supported	5.0.0

4	32	Undeliverable-mail-physical-delivery-address-incorrect	5.0.0
4	33	Undeliverable-mail-physical-delivery-office-incorrect-or-invalid	5.0.0
4	34	Undeliverable-mail-physical-delivery-address-incomplete	5.0.0
4	35	Undeliverable-mail-recipient-unknown	5.0.0
4	36	Undeliverable-mail-recipient-deceased	5.0.0
4	37	Undeliverable-mail-organisation-expired	5.0.0
4	38	Undeliverable-mail-recipient-refused-to-accept	5.0.0
4	39	Undeliverable-mail-recipient-did-not-claim	5.0.0
4	40	Undeliverable-mail-recipient-changed-address-permanently	5.0.0
4	41	Undeliverable-mail-recipient-changed-address-temporarily	5.0.0
4	42	Undeliverable-mail-recipient-changed-temporary-address	5.0.0
4	43	Undeliverable-mail-new-address-unknown	5.0.0
4	44	Undeliverable-mail-recipient-did-not-want-forwarding	5.0.0
4	45	Undeliverable-mail-originator-prohibited-forwarding	5.0.0
8	46	Secure-messaging-error	5.7.0
1	47	Unable-to-downgrade	5.6.5
0	48	Unable-to-complete-transfer	5.5.0
0	49	Transfer-attempts-limit-reached	5.4.0
1	50	Incorrect-notification-type	5.6.0
8	51	Dl-expansion-prohibited-by-security-policy	5.7.2
8	52	Forbidden-alternate-recipient	5.7.0
8	53	Security-policy-violation	5.7.0
8	54	Security-services-refusal	5.7.0
8	55	Unauthorised-dl-member	5.7.0
8	56	Unauthorised-dl-name	5.7.2
8	57	Unauthorised-originally-intended-recipient-name	5.7.0
8	58	Unauthorised-originator-name	5.7.1
8	59	Unauthorised-recipient-name	5.7.0
8	60	Unreliable-system	5.7.3

8	61	Authentication-failure-on-subject-message	5.7.7
8	62	Decryption-failed	5.7.5
8	63	Decryption-key-unobtainable	5.7.5
8	64	Double-envelope-creation-failure	5.7.0
8	65	Double-enveloping-message-restoring-failure	5.7.0
8	66	Failure-of-proof-of-message	5.7.0
8	67	Integrity-failure-on-subject-message	5.7.0
8	68	Invalid-security-label	5.7.0
8	69	Key-failure	5.7.5
8	70	Mandatory-parameter-absence	5.7.0
8	71	Operation-security-failure	5.7.0
8	72	Repudiation-failure-of-message	5.7.0
8	73	Security-context-failure	5.7.0
8	74	Token-decryption-failed	5.7.5
8	75	Token-error	5.7.0
8	76	Unknown-security-label	5.7.0
8	77	Unsupported-algorithm-identifier	5.7.4
8	78	Unsupported-security-policy	5.7.4

Appendix C: Examples for Messages and Reports

C1. Delivered Message with text attachment

Delivered Message (M_5K00AG0HBDM0F2F9.OUT)

To: "G=MG1;S=MGATE;CN=MG1 MGATE;O=TEST;A=VIAT;C=DE" <49603@viaT.de>
From: "G=ipm;S=tester;O=test;A=viaT;C=de" <1045@viaT.de>
Message-ID: 615 10/11/13
X-MPDUID: 3D23437A11DCEC31170084BF
Date: 13 Nov 2010 13:10:22 +0100
Subject: Test mit Textbodypart
Disposition-Notification-To: "G=ipm;S=tester;O=test;A=viaT;C=de"
MIME-Version: 1.0
Content-Type: text/plain
Content-Transfer-Encoding: 8bit

Test
äöüÄÖÜß12345678901234567890123456789012345678901234567890123456789
2345678901234567890123456789012345678901234567890123456789012345678901234567890
1234567890123456789012345678901234567890123456789012345678901234567890123456789
0123456789012345678901234567890123456789012345678901234567890

For this message (filename M_5K00AG0HBDM0F2F9.OUT) a receipt notification is requested but not sent (see following examples for Reports)

C2. Delivered Message with binary attachment

Delivered Message (M_5K00AG0HBDM0F2FA.OUT)

To: "G=MG1;S=MGATE;CN=MG1 MGATE;O=TEST;A=VIAT;C=DE" <49603@viaT.de>
From: "G=ipm;S=tester;O=test;A=viaT;C=de" <1045@viaT.de>
Message-ID: 616 10/11/13
X-MPDUID: 575BCBFB11DCEB9F1700C184
Date: 13 Nov 2010 13:10:22 +0100
Subject: Test mit Binäranhang
Disposition-Notification-To: " G=ipm;S=tester;O=test;A=viaT;C=de "
MIME-Version: 1.0
Content-Type: application/octet-stream
Content-Disposition: attachment; filename="4d654d1d.zip"
Content-Transfer-Encoding: binary

PK□□□ □ tYr2ÄQa6÷□ ‹□
.
.
.
□ ¶□ 4d654d1d.0PK□□ □ □ 8 □

For this message (filename M_5K00AG0HBDM0F2FA.OUT) a receipt notification is requested and a Non Receipt Notification was sent (see following examples for Reports)

C3. Delivered Message with Multiple attachments

Delivered Message (M_5K00AG0HBDM0F2F8.OUT)

To: "G=MG1;S=MGATE;CN=MG1 MGATE;O=TEST;A=VIAT;C=DE" <49603@viaT.de>
From: "G=ipm;S=tester;O=test;A=viaT;C=de" <21046@viaT.de>
Message-ID: 614 10/11/13
X-MPDUID: 8B0663A011DCEC4417009682
Date: 13 Nov 2010 13:10:22 +0100
Subject: Test mit 3 Bodyparts
Disposition-Notification-To: "G=ipm;S=tester;O=test;A=viaT;C=de"
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="MG_=_CA610D0211DC91E900007CAD_=_MG"

--MG_=_CA610D0211DC91E900007CAD_=_MG
Content-Type: text/plain
Content-Transfer-Encoding: 8bit

Test äöüÄÖÜß

--MG_=_CA610D0211DC91E900007CAD_=_MG
Content-Type: application/octet-stream
Content-Disposition: attachment; filename="4d654d1d.zip"
Content-Transfer-Encoding: binary

PK□□□ □ tYr2ÄQa6÷□ ‹□4d654d1d.0µ“ls£:□…÷Tñ¨ê¥Ói3xJU/$!¦DØb2xgd□°1Ø
.
.
.
□ ¶□ 4d654d1d.0PK□□ □ □ 8 □
--MG_=_CA610D0211DC91E900007CAD_=_MG
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from url=(0062)https://securep7.viat-test.de/~0000001045/result/fetch_all.RES -->
<HTML><HEAD>
<META http-equiv=Content-Type content="text/html; charset=windows-1252">
<META content="MSHTML 5.50.4930.1700" name=GENERATOR></HEAD>
<BODY><XMP>LOGIN::
.
.
.
</XMP></BODY></HTML>
□
--MG_=_CA610D0211DC91E900007CAD_=_MG—

For this message (filename M_5K00AG0HBDM0F2F8.OUT) a receipt notification is requested and a Receipt Notification was sent (see following examples for Reports).

C4. Delivered Message with Multirecipient

To: "G=edi;S=tester;O=dtag;A=viat-test;C=de" <21047@viaT.de>
To: "G=ipm;S=tester;CN=ipm tester;O=DTAG;A=viat-test;C=DE" <21046@viaT.de>
Cc: "G=ipm;S=testmiv;O=dtag;A=viat-test;C=de" <23998@viaT.de>
Cc: "G=EDI;S=TESTMIV;CN=EDI TESTMIV;O=DTAG;A=VIAT-TEST;C=DE" <23999@viaT.de>
Cc: "S=murxer;O=murx;A=viat-test;C=de" <X@viaT.de>
Bcc: "G=MG1;S=MGATE;CN=MG1 MGATE;O=DTAG;A=VIAT-AS2;C=DE" <49603@viaT.de>
From: "G=MG1;S=MGATE;CN=MG1 MGATE;O=DTAG;A=VIAT-AS2;C=DE" <49603@viaT.de>
Message-ID: MGATE 0001 11/03

X-MPDUID: 5758CA1B11E0498E00005292
Date: 8 Mar 2011 14:14:12 +0100
Subject: test Multi Recipients
MIME-Version: 1.0
Content-Type: text/plain
Content-Transfer-Encoding: 8bit

test

The message has been sent to seven recipients and the own MessageGate account was addressed as a Blind carbon copy recipient.

C5. Submitted Message and no Report Request

Submitted Message (M_Test_3_Body010.IN)

To: "" <21046@viat.de>
Subject: test 3 ohne Leerzeile Bodyparts
Message-Id: 260001 12/11/10 MGATE Test
Date: Tue, 12 Nov 2010 13:16:24 +0100
MIME-Version: 1.0
Content-Type: multipart/mixed;
	boundary="----=_NextPart_000_0007_01C7E331.7A0CA460"
Content-Transfer-Encoding: binary

------=_NextPart_000_0007_01C7E331.7A0CA460
Content-Type: text/plain;
	charset="iso-8859-1"
Content-Transfer-Encoding: 7bit

------=_NextPart_000_0007_01C7E331.7A0CA460
Content-Type: application/x-pkcs12;
	name="hpm-webdav.p12"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
	filename="hpm-webdav.p12"

MIIKAQBAzCCCccGCSqGSIb3DQEHAaCCCbgEggm0MIIJsDCCBGcGCSqGSIb3DQEHBqCCBFgwggRU
AgEAMIIETQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQIzN9gMIQvocsCAggAgIIEILQGaNZr
0IW6bN6jEdpthjnBzmCv8W9ipvE8wmpVxzUEwj5Mh226vHaBp2WtMBaHPSomsXFMPEJJj9JFnF2S
gPxDZVjUe5lmUB2EQDAopQEYLxJSX0YXh8uqnSD5Se4vuex+kunnb6o2nGXT8+Y9m3/uNCD9MEb6
CGIA0JExtmWQJXkDeHDZjLjYiVCpcItNeMNc7EGH842jRGzS1umfOeSWb8+TcA2/uZtzaE9uIL7I
LfD7dflJz/4uawC+LstCfO984pFKR8vOxKlAdbOn1CpuSIQFHHdgCZYVy1EHOdlImQbmI+bJ2Gwx
UPKDdUGdyK6G45JHZjuj4zDUSRXwfnrRmSUHAMZhUpRQwApPYyQo6zxhdd7NsdxPu7mDisNE/p6p
0DNPTf97j/AiPWVMEwz0nsfITqF+4L0NXVKia7Mp8o7Zzrn5XpwJ0/LP+47/+ZyCaClqB/qYtGlb
xlgI04DFbS6xaoUu7iNh7ZSqnXNMRJREtBx/WVoMChpYHuvVqitPWdsBpawNpUHs5uEXUopa0Uly
XOn9ALfLE0t9v5FP4NE3xSHMPGSAc5iisH7Fys8g5Z+SGp3n9ynM8Jw97JhZfjKoQMqrMFzNL5Fl
ZUBVwNYOtUNXxKJ3L+1WtRXSEQgmfhptKZicCZKHoGZQ4Z8F4r9sA7wmS9CbLjiNQlmWlrvaMWE3
fi6dzhrUOFIdu2LE7Tl7+1Qmh/AcP3NVlUSUZlGJqqGc5I1BUpMP3CJPo25xJ7zAek/YECJmQ5p9
l+c2Ja60suKAlt6VfBcd747nIEQXdxYvI8cXQeuzhVmvbBrX12Hg4ISioygEg5XFsd4DutZAxTuw
gReDf8Hw/rMQfE6fhHiIS7YirkqJt+q53uILMuN4sdV6u+nFsaoRYT84vTJZ30B5WsH3Zs4T47r1
rTCn/BpQoQ8N62QF9zAPPL5AfctnDw/oZahJUqnQUNW7H86dLJ1ZkPJElCQ9quQSvjcMWZviliyr
lnyeW0JE53V5N/38me3xV89f6iUkNvWg3catzHTH5Bay1E1NGVi9cYfuNJ+qsHMxegcu5h9UGiVX
Z6AFQ5TOwPrObyOunVjUsGT8yIlcpHEBwilPFP4GXq30gt3H7S2sDZSbrrDUYeWgJBgwmJaEjo/z
Pl67psBqnh4HKZoXAKSrfcF2JK2nt6q442tplREVpkTXFGF6p7nqVvnP4RBD2LbFD/uzBxpchjR3
62I6LZ75qjSf4hZHnAVCD7BtfPx3j3mg8fICp7ZyGRgSARpaLrYoMzbMXgIPFYUOqf8rug/AoCqB
SD6OvMtvRfn5c3JceC9IZQ3/LGaqx7RGaUHYJaSXHPrFCiozxtt2slw5nhWlFF1fgfJqVf2L41E2
8f7pRyHPejTBK1tozyHaWvsTm7kFm8FliDCCBUEGCSqGSIb3DQEHAaCCBTIEggUuMIIFKjCCBSYG
CyqGSIb3DQEMCgECoIIE7jCCBOowHAYKKoZIhvcNAQwBAzAOBAiZFPkQkLYL2wICCAAEggTIcJfj
y/4rcNs13Bxzac5e9bbDPqW6l6Cng7jB6vXjSPBNNMLL+7BcVKeSIWupmsQeQkvZGhdcby7Najsk
KE0EmaVVUPo1IgACKvZ2dc6nAVEeHbA14N1Zl2gCrvKZb1WHWj6NJ9e1xAKYzahVb5dkFNQIO8Y8
dQXgYhJF6davx+nFdhnoo8wnOA8ntwpJggGJAw5xM7GLlV2Xy0wahfoKG53Jxwgsz/OiLX/uh/Vk
c/kO+nKF4/au5igH9eI8M6/I7A6kP854eXuMDWPXQHE35xAXrvt3gQd1D1n2wMGt/RyCDA1h4mNr

XwheqI3nPScmwtRRsC6JSxZ1dx3kr4Zrw7yRR9HjT7oCn5VjonsdMfEATqY1GLDKOw4LE30Za3bW
kVSl3VzLxZx80WLcdiL9R1tn1FMbh/YJFs52OCF1MqnZdKq/fEP6yUK260Pl6mZCS1FLTHI00vN3
+WPY8itoVb5qqPEHNCh1Li3mCHHv7hLS9t6p+JM4+/y2G6MD8pPp/dnUxSidpbgIPV9/DQAMcx9P
PgHX01HnF8b8r61sKZX0KzizxjdxTSdur/A5ZVDtZBzM2etFcEt17O08tko31UmAC/XWe9p2mjA1
ft2NAM3Yqyjf03zT7jw4uLskwcniPcd0snbvlUY7prvn/7oBuTzklqmtvf9nfziyhNjByeIytJyc
qqE8Q+MplrbbWoUnQ2S1cg9zz38EVBIAt6WGYvgsKeDAt1Ix1ZyoI2InaCs4cXnZRR9HLZXL2hTW
aPZ7BVRtYohdme/18XtJgzySggdAMqxOG3I+JiqXXa4M3a38TrndEjNzY9pHLa6Pi1R3IiBZ4ZiB
Ayo2Z42HiU83ZAsDxYTPbb2oYHgzijbvCQ7WOmhefhTTV/q5S89FOEtlabYrjBdPliI+Q4GiPYin
Aw/BgDThhkx5FXZz8L8WTTwnlvZ0OXq6tQ9ZfiNblZJYth/C/pjSf2kLUH/bj8X8RHeXv3DfaOkn
brqyx401gwIPx2JSpqcxX7kHroVxF+lYEHpfeEaTJ/650V3yUXmKAwL/CNxOhEqIj6QlpfPRAzb7
kqDFFX1Y/cVTkYQGs7tHMVFFiEvn93MVri0hIReDxTElhOQ6a/8D/laitiNO9nF4zATVI7nuIxkg
I2NU3iJMqrXNlpgnh63Z8phS74Q6RW5O8DtVXFDBVNvIFiMUvBYxdt8bPLi/c9ZrXFjTr5ozSn2h
4WSKCiRpDfZGU+u9a4Tr+sU8GZyrDf8QnOB0sUo6aqF3Bjbb2jUHqRgVX1UgmeDGuTZSW2qZY2DQ
HIJMC7E1BjmVsyPIodJLFRN8hBZCseJwuQ/6dtDoITsrbPtFTNN2kvtpgly6voQYoIDWTyWxFCB8
NE3hyhkeTtVB92VQ3hxPGvgAp2yboIxKKnoBBrvDSpyawB/a629Op3a1NO82A6w6JwFVjOUvURSj
PovxBSACQtxr/dPAEuZIGNyftqHpWbO01CeISvKJ6VnoPYh6R2AJwWgDGPVqdBRuSVIWq4PDasTG
8yUCWqdfYFGsbbTMyDy0n5vzHmSlg1Z/3w7nU4ze+aIRRB+xRJiBUBzi+An1qUCwHk9tMa9lqNWc
1wct6024js0/wocPpq7kVKBD2zf9Uy4KMSUwIwYJKoZIhvcNAQkVMRYEFA73TcSOycMboZppjFUR
sioIKUFCMDEwITAJBgUrDgMCGgUABBTl7cq0AOvHFv4Aixdzm1d/1GaKNgQIUQPUr3fqiCICAggA

```
------=_NextPart_000_0007_01C7E331.7A0CA460
Content-Type: application/octet-stream;
        name="dtag-06.mod"
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment;
        filename="dtag-06.mod"

[Modul]
Name = "DTAG-06"
Bemerkung = "DTAG-Reservemodul"
Zielverzeichnis = "DTAG"
Ueberschreiben = 0
Delete = 1
Betreff_auswerten = 1
CASE_SENSITIVE = 1
Absender = "S=KUNDENBUCHHALTUNG;O=DTAG;A=viaT;C=DE"
EXAKT_auswerten = 0
[Subject]
Start1 = 1
Text1 = "DTAG__>>$06"
[File]
[Message]
K1Type = Betreff
K1Start = 23
K1Laenge = 8
K2Type = Fest
K2Wert = ".Z"
K3Type = Betreff
K3Start = 32
K3Laenge = 2
[Text]

------=_NextPart_000_0007_01C7E331.7A0CA460—
```

In this message no report was requested so the Status “Sent” will not change until the entry is purged in the database (see following examples for Reports).

C6. Submitted Message with Report Request

Submitted Message (M_Test_3_Body011.IN)

```
To: "" <21046@viat.de>
Subject: test 3 Bodyparts
Message-Id: 260002 12/11/10 MGATE Test
Date: Tue, 12 Nov 2010 14:46:24 +0100
```

```
Disposition-Notification-To: ""
MIME-Version: 1.0
Content-Type: multipart/mixed;
      boundary="----=_NextPart_000_0007_01C7E331.7A0CA460"
Content-Transfer-Encoding: binary

------=_NextPart_000_0007_01C7E331.7A0CA460
Content-Type: text/plain;
      charset="iso-8859-1"
Content-Transfer-Encoding: 7bit


------=_NextPart_000_0007_01C7E331.7A0CA460
Content-Type: application/x-pkcs12;
      name="hpm-webdav.p12"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
      filename="hpm-webdav.p12"

MIIKAQIBAzCCCccGCSqGSIb3DQEHAaCCCbgEggm0MIIJsDCCBGcGCSqGSIb3DQEHBqCCBFgwggRU
.
.
.
sioIKUFCMDEwITAJBgUrDgMCGgUABBTl7cq0AOvHFv4Aixdzm1d/1GaKNgQIUQPUr3fqiCICAggA

------=_NextPart_000_0007_01C7E331.7A0CA460
Content-Type: application/octet-stream;
.
.
.
[Text]

------=_NextPart_000_0007_01C7E331.7A0CA460—
```

In this message a report (it is not necessary to write an X.400 address between quotation marks) was requested and based on the parameter in the Profile (Value is 2) this request is mapped into an X.400 Receipt Notification request. The status of the message will change when the report arrives (see following examples for Reports).

C7. Submitted Message with Multirecipient

```
To: " G=ipm;S=tester;O=test;A=viaT;C=de " <x@viaT.de>
to: "" <41040@viat.de>
CC: "G=edi;S=tester;O=test;A=viaT;C=de " <x@viaT.de>
cc: "" <31044@viat.de>
cc: " c=de; a=viat; o=unknown; S=dummy " <x@viat.de>
cc: "" <70000@viat.de>
BCC: "" <49603@viat.de>
Message-ID: MGATE 0001 11/03/07
Date: 07 March 2011 10:56:05 +0100
Subject: test Multi Recipients
Disposition-Notification-To: ""
MIME-Version: 1.0
Content-Type: text/plain
Content-Transfer-Encoding: 8bit

Test
```

The message has been sent to seven recipients and it is not relevant whether capital or small letters are used for the address type. The own MessageGate account was addressed as a Blind carbon copy recipient.

C8. Transmission set with two Interchanges

Submitted Transmission set file T_TestEDI_018.IN

```
UNA:+.? '
UNB+UNOA:2+MGATE1:65+TESTER:65+020508:1413+0709210008'
UNH+EVA0000001+INVOIC:D:95A:UN:ETEIB++0'
BGM++D--01/333700001003'
DTM+003:20080729'
DTM+263:9512:609'
NAD+II+++NL 2 STUTTGART-NORD+10 02 00+STUTTGART-NORD++70191+IC'
COM+0711/555-5002:TE'
COM+0711/555-5555:FX'
NAD+IV++TBX::FGNR 10110::93606 TESTHEIM'
CUX+1:DEM'
LIN+1++333700001003:ISN:DT6:DTC++0'
LIN+2+++1:1+1'
MOA+203:0.2086'
LOC+1+33XXX:::TESTUNION'
QTY+107:2'
DTM+163:20080619090423:204'
DTM+048:131:807'
LIN+3+++1:1+1'
MOA+203:0.3129'
LOC+1+31XXX:::TESTUNION'
QTY+107:3'
DTM+163:20080626091536:204'
DTM+048:192:807'
LIN+4+++1:1+1'
MOA+203:0.1043'
LOC+1+9193XXX:::TESTUNION'
QTY+107:1'
DTM+163:20080711080945:204'
DTM+048:51:807'
LIN+5+++1:1+1'
MOA+203:0.1043'
LOC+1+9193XXX:::TESTUNION'
QTY+107:1'
DTM+163:20080711095040:204'
DTM+048:27:807'
UNS+S'
MOA+079:0.7301'
UNT+37+EVA0000001'
UNZ+1+0709210008'
```

```
UNA:+.? '
UNB+UNOA:2+MGATE1:65+TESTER:65+020508:1413+0709210009'
UNH+EVA0000001+INVOIC:D:95A:UN:ETEIB++0'
BGM++D--01/333700001003'
DTM+003:20080729'
DTM+263:9512:609'
NAD+II+++NL 2 STUTTGART-NORD+10 02 00+STUTTGART-NORD++70193+IC'
COM+0711/555-5002:TE'
COM+0711/555-5555:FX'
NAD+IV++TBX::FGNR 10110::93606 TESTHEIM'
CUX+1:DEM'
LIN+1++333700001003:ISN:DT6:DTC++0'
LIN+2+++1:1+1'
MOA+203:0.2086'
LOC+1+33XXX:::TESTUNION'
QTY+107:2'
DTM+163:20080619090423:204'
DTM+048:131:807'
LIN+3+++1:1+1'
MOA+203:0.3129'
LOC+1+31XXX:::TESTUNION'
QTY+107:3'
DTM+163:20080626091536:204'
DTM+048:192:807'
LIN+4+++1:1+1'
MOA+203:0.1043'
LOC+1+9193XXX:::TESTUNION'
QTY+107:1'
DTM+163:20080711080945:204'
DTM+048:51:807'
LIN+5+++1:1+1'
MOA+203:0.1043'
LOC+1+9193XXX:::TESTUNION'
QTY+107:1'
DTM+163:20080711095040:204'
DTM+048:27:807'
UNS+S'
MOA+079:0.7301'
UNT+37+EVA0000001'
UNZ+1+0709210009'
```

The file may contain an empty line to separate the Interchanges, but this is not necessary.

C9. Status Report without History

Request Status report (S_*.IN)

Since: 13-Nov-2010
Direction: both

Status report (S_*.OUT)

Status Report for UserID 49603; generated 13-NOV-2010 14:56:23
Filters: Disposition=All, Direction=Both, Format=Actual, Since=13-Nov-2010

From: " G=ipm;S=tester;O=test;A=viaT;C=de" 21046@viaT.de
Order-ID: 5K00AG0HBDM0F2F8
Message-ID: 614 10/11/13
MTS-ID: CA610D0211DC91E900007CAD
Status: Read
Date: 13-Nov-2010 14:01:18 +0100

From: " G=ipm;S=tester;O=test;A=viaT;C=de " 21046@viaT.de
Order-ID: 5K00AG0HBDM0F2F9
Message-ID: 615 10/11/13
MTS-ID: CA79C90011DC91E900007EAD
Status: Received
Date: 13-Nov-2010 13:10:23 +0100

From: "G= G=ipm;S=tester;O=test;A=viaT;C=de " 21046@viaT.de
Order-ID: 5K00AG0HBDM0F2FA
Message-ID: 616 10/11/13
MTS-ID: CA9FC7DB11DC91E900007EAD
Status: Denied: (Reason: 0, Diagnostic: 0))
Date: 13-Nov-2010 14:01:18 +0100

To: "" 21046@viaT.de
Order-ID: Test_3_Body010
Message-ID: 260001 12/11/10 MGATE Test
MTS-ID: 71F6370611DC91EB0000DDAE
Status: Sent
Date: 13-Nov-2010 13:22:12 +0100

To: "c=de;a=viat;s=nicht_vorhanden,o=test" X@viaT.de
Order-ID: NDN001
Message-ID: MGATE 49603 00001 13112010
MTS-ID: MGate<5K00AG0HBDM208B4>
Status: Error: (Reason: 159416490, Diagnostic: 0)
Date: 13-Nov-2010 13:22:13 +0100

To: "c=de;a=viat;s=nicht-vorhanden,o=test" X@viaT.de
Order-ID: NDN002
Message-ID: MGATE 49603 00002 13112010
MTS-ID: D1FC163311DC91F400007EBA
Status: Failed: (Reason: 6, Diagnostic: 0)
Date: 13-Nov-2010 14:29:25 +0100

To: "" 21046@viaT.de
Order-ID: Test_3_Body011
Message-ID: 260002 12/11/10 MGATE Test
MTS-ID: 098FC66111DC91F80000A6BD
Status: Read
Date: 13-Nov-2010 14:54:00 +0100

This status report shows the status of different messages. To limit the number of entries in the report only those were selected which were sent or received since the 13th of November 2010.

The first message was received, a receipt report was requested and was sent → Status is Read

The second message was received but no receipt report was requested. The sender only receives a delivery report if he had requested it → Status is Received

The third message was received, a receipt report was requested and a negative report was sent → Status is Denied

The fourth message was sent and no report was requested. Hence the status remains “Sent” until the entry is purged. There will be no information if the delivery of the message had failed → Status is Sent

The fifth message was not sent because there is an invalid character in the address element (in “s=” the character “_” is used) that cause a process error → Status is Error.

The sixth message was sent and a report was requested. The message has an invalid “TO:” address and the MTA generated a Non Delivery Notification → Status is Failed.

The seventh message was delivered to a partner and a receipt notification was sent back → Status is Read.

C10. Status Report with History

Request Status report (S_*.IN)

Format: History
Direction: both

Status report (S_*.OUT)

Status Report for UserID 49603; generated 13-NOV-2010 14:56:22
Filters: Disposition=All, Direction=Both, Format=History

From: " G=ipm;S=tester;O=test;A=viaT;C=de " 21046@viaT.de
Order-ID: 5K00AG0HBDM0F2F8
Message-ID: 614 10/11/13
MTS-ID: CA610D0211DC91E900007CAD
Received: 13-Nov-2010 13:10:22 +0100
Read: 13-Nov-2010 14:01:18 +0100

From: " G=ipm;S=tester;O=test;A=viaT;C=de " 21046@viaT.de
Order-ID: 5K00AG0HBDM0F2F9
Message-ID: 615 10/11/13
MTS-ID: CA79C90011DC91E900007EAD
Received: 13-Nov-2010 13:10:23 +0100

From: " G=ipm;S=tester;O=test;A=viaT;C=de " 21046@viaT.de
Order-ID: 5K00AG0HBDM0F2FA
Message-ID: 616 10/11/13
MTS-ID: CA9FC7DB11DC91E900007EAD
Received: 13-Nov-2010 13:10:23 +0100
Denied: 13-Nov-2010 14:01:18 +0100 (Reason: 0, Diagnostic: 0)

To: "" 21046@viaT.de
Order-ID: Test_3_Body010
Message-ID: 260001 12/11/10 MGATE Test
MTS-ID: 71F6370611DC91EB0000DDAE
Sent: 13-Nov-2010 13:22:12 +0100

To: "c=de;a=viat-test;s=nicht_vorhanden,o=test" X@viaT.de
Order-ID: NDN001
Message-ID: MGATE 49603 00001 13112010
MTS-ID: MGate<5K00AG0HBDM208B4>
Error: 13-Nov-2010 13:22:13 +0100 (Reason: 159416490, Diagnostic: 0)

To: "c=de;a=viat-test;s=nicht-vorhanden,o=test" X@viaT.de
Order-ID: NDN002
Message-ID: MGATE 49603 00002 13112010
MTS-ID: D1FC163311DC91F400007EBA
Sent: 13-Nov-2010 14:29:19 +0100

Failed: 13-Nov-2010 14:29:25 +0100 (Reason: 6, Diagnostic: 0)

To: "" 21046@viaT.de
Order-ID: Test_3_Body011
Message-ID: 260002 12/11/10 MGATE Test
MTS-ID: 098FC66111DC91F80000A6BD
Sent: 13-Nov-2010 14:52:21 +0100
Delivered: 13-Nov-2010 14:52:27 +0100
Read: 13-Nov-2010 14:54:00 +0100

This status reports shows the status history of different messages:

The first message was received and a receipt report was sent at 14:01

The second message was received at 13:10 but no receipt report was requested. The sender only received a delivery report because he had requested it

The third message was received at 13:10, a receipt report was requested and negative report was sent → Status is Denied

The fourth message was sent at 13:22 and no report was requested. Hence the status remains “Sent” until the entry is purged. There will be no information if the delivery of the message has failed.

The fifth message was not sent because there is an invalid character in the address element (in “s=” the character “_” is used) that cause a process error → Status is Error.

The sixth message was sent at 14:29 and a report was requested. The message has an invalid “To:” address and the MTA generated a Non Delivery Notification.

The seventh message was sent at 14:52, delivered to partner at 14:52 and a receipt notification was generated and sent back at 14:54.

C11. Status Report for a selected Order-ID

Request Status report (S_*.IN)

Order-ID: NDN002

Status report (S_*.OUT)

Status Report for UserID 49603; generated 13-NOV-2010 14:57:22

Filters: Disposition=All, Direction=Sent, Format=Actual, Order-ID=NDN002

To: "c=de;a=viat;s=nicht-vorhanden,o=test" X@viaT.de

Order-ID: NDN002

Message-ID: MGATE 49603 00002 13112010

MTS-ID: D1FC163311DC91F400007EBA

Status: Failed: (Reason: 6, Diagnostic: 0)

Date: 13-Nov-2010 14:29:25 +0100

This status reports shows the status of a message, which was selected using the Parameter Order-ID.

C12. Status Report for a selected Message-ID

Request Status report (S_*.IN)

Message-ID: 2600*

Status report (S_*.OUT)

Status Report for UserID 49603; generated 13-NOV-2010 14:58:21
Filters: Disposition=All, Direction=Sent, Format=Actual, Message-ID=2600*

To: "" 21046@viaT.de
Order-ID: Test_3_Body010
Message-ID: 260001 12/11/10 MGATE Test
MTS-ID: 71F6370611DC91EB0000DDAE
Status: Sent
Date: 13-Nov-2010 13:22:12 +0100

To: "" 21046@viaT.de
Order-ID: Test_3_Body011
Message-ID: 260002 12/11/10 MGATE Test
MTS-ID: 098FC66111DC91F80000A6BD
Status: Read
Date: 13-Nov-2010 14:54:00 +0100

This status report shows the status of two messages, which were selected using the Parameter Message-ID and using a wildcard as part of this ID.

C13. Status Report for denied Messages

Request Status report (S_*.IN)

Format: History
Direction: both

Status report (S_*.OUT)

Status Report for UserID 49603; generated 15-NOV-2010 16:21:04
Filters: Disposition=All, Direction=Both, Format=History

From: " G=ipm;S=tester;O=test;A=viaT;C=de " 21046@viaT.de
Order-ID: T730AG0HBFP1BBC0
Message-ID: 625 10/11/15
MTS-ID: 76CEBBE911DC93960000819A
Error: 15-Nov-2010 13:37:25 +0100 (Reason: 1, Diagnostic: 17)

From: " G=ipm;S=tester;O=test;A=viaT;C=de " 21046@viaT.de
Order-ID: T730AG0HBFP1BBC1
Message-ID: 626 07/11/15
MTS-ID: 7748EA6D11DC93960000889A
Error: 15-Nov-2010 15:11:57 +0100 (Reason: 1, Diagnostic: 11)

From: "G G=ipm;S=tester;O=test;A=viaT;C=de " 21046@viaT.de

Order-ID: T730AG0HBFP1BBC3
Message-ID: 628 10/11/15
MTS-ID: 77AC72F911DC939600008A9A
Received: 15-Nov-2010 16:18:57 +0100

This status report shows the status of messages which are not delivered to a users directory because of partnership errors (central EDI function).

In the first message a wrong recipient ID was found in the header of the EDIFACT interchange. The MTA has created a Non Delivery Notification with a Diagnostic code “No-bilateral-agreement” (17) and has sent it to the the sender of the message.

In the second message there is a wrong value in the UNZ of the EDIFACT interchange. The MTA has created a Non Delivery Notification with a Diagnostic code “Invalid-arguments” (11) and has sent it to the sender of the message.

The third message was delivered to the directory at 16:18.

C14. Report for submitted message (Multirecipient)

Status Report for UserID 49603; generated 8-Mar-2011 11:37:06 +0100
Filters: Disposition=All, Direction=Both, Format=History

To: "G=ipm;S=tester;O=test;A=viaT;C=de" <x@viaT.de>
Order-ID: Test_ISOTEXT_M018
Message-ID: MGATE 0001 11/03/07
MTS-ID: A2CD418E11E048A90000D680
Sent: 7-Mar-2011 10:57:03 +0100
Delivered: 7-Mar-2011 11:39:44 +0100

To: "" <41040@viat.de>
Order-ID: Test_ISOTEXT_M018
Message-ID: MGATE 0001 11/03/07
MTS-ID: A2CD418E11E048A90000D680
Sent: 7-Mar-2011 10:57:03 +0100
Delivered: 7-Mar-2011 11:39:44 +0100

Cc: "G=edi;S=tester;O=test;A=viaT;C=de" <x@viaT.de>
Order-ID: Test_ISOTEXT_M018
Message-ID: MGATE 0001 11/03/07
MTS-ID: A2CD418E11E048A90000D680
Sent: 7-Mar-2011 10:57:03 +0100
Delivered: 7-Mar-2011 11:39:44 +0100
Read: 7-Mar-2011 15:11:38 +0100

Cc: "" <31044@viat.de>
Order-ID: Test_ISOTEXT_M018
Message-ID: MGATE 0001 11/03/07
MTS-ID: A2CD418E11E048A90000D680
Sent: 7-Mar-2011 10:57:03 +0100

Failed: 7-Mar-2011 10:57:03 +0100 (Reason: 1, Diagnostic: 11)

Cc: "c=de; a=viat; o=unknown; S=dummy" <x@viat.de>
Order-ID: Test_ISOTEXT_M018
Message-ID: MGATE 0001 11/03/07
MTS-ID: A2CD418E11E048A90000D680
Sent: 7-Mar-2011 10:57:03 +0100
Failed: 7-Mar-2011 10:57:03 +0100 (Reason: 6, Diagnostic: 0)

Cc: "" <70000@viat.de>
Order-ID: Test_ISOTEXT_M018
Message-ID: MGATE 0001 11/03/07
MTS-ID: A2CD418E11E048A90000D680
Error: 7-Mar-2011 10:57:03 +0100 (Reason: 6, Diagnostic: 0)

Bcc: "" <49637@viat.de>
Order-ID: Test_ISOTEXT_M018
Message-ID: MGATE 0001 11/03/07
MTS-ID: A2CD418E11E048A90000D680
Sent: 7-Mar-2011 10:57:03 +0100
Delivered: 7-Mar-2011 11:39:44 +0100

The Order-ID and the Message-ID are identical for all entries. Only the MTS-ID might be different because in case of an error the MessageGate process will create this ID and not the MTA. These entries are only unambiguous in conjunction with a specific recipient address. In this example all address types (To:, Cc: and Bcc.) were used and for some of these recipient addresses a Non Delivery Notification has been received.

The 4th recipient is an EDIBOX that supports only messages with one recipient and EDIFACT document → Error “Invalid arguments”.

The 5th recipient has a wrong X.400 address → Error “Unknown User“

The 6th recipient has an invalid User-ID → Error “Unknown User“

Appendix D: Character sets

Printable String:

A, B…Z	Capital letter
a, b…z	Small letter
0, 1…9	Number
“ “	Space
'	Apostrophe
(	Left Parenthesis
)	Right Parenthesis
+	Plus sign
-	Hyphen - Minus
,	Comma
.	Full stop
/	Solidus
:	Colon
=	Equal sign
?	Question mark

ISOLatin 1 (ISO 8859-1)

Decimal	Hexadecimal	Character
32	0x20	Space
33	0x21	!
34	0x22	
35	0x23	#
36	0x24	$
37	0x25	%
38	0x26	&
39	0x27	'
40	0x28	(
41	0x29	)
42	0x2A	*
43	0x2B	+
44	0x2C	,

45	0x2D	-
46	0x2E	.
47	0x2F	/
48	0x30	0
49	0x31	1
50	0x32	2
51	0x33	3
52	0x34	4
53	0x35	5
54	0x36	6
55	0x37	7
56	0x38	8
57	0x39	9
58	0x3A	:
59	0x3B	;
60	0x3C	<
61	0x3D	=
62	0x3E	>
63	0x3F	?
64	0x40	@
65	0x41	A
66	0x42	B
67	0x43	C
68	0x44	D
69	0x45	E

70	0x46	F
71	0x47	G
72	0x48	H
73	0x49	I
74	0x4A	J
75	0x4B	K
76	0x4C	L
77	0x4D	M
78	0x4E	N
79	0x4F	O
80	0x50	P
81	0x51	Q
82	0x52	R
83	0x53	S
84	0x54	T
85	0x55	U
86	0x56	V
87	0x57	W
88	0x58	X
89	0x59	Y
90	0x5A	Z
91	0x5B	[
92	0x5C	\
93	0x5D	]
94	0x5E	^

95	0x5F	_
96	0x60	`
97	0x61	a
98	0x62	b
99	0x63	c
100	0x64	d
101	0x65	e
102	0x66	f
103	0x67	g
104	0x68	h
105	0x69	i
106	0x6A	j
107	0x6B	k
108	0x6C	l
109	0x6D	m
110	0x6E	n
111	0x6F	o
112	0x70	p
113	0x71	q
114	0x72	r
115	0x73	s
116	0x74	t
117	0x75	u
118	0x76	v
119	0x77	w

120	0x78	x
121	0x79	y
122	0x7A	z
123	0x7B	{
124	0x7C	|
125	0x7D	}
126	0x7E	~
161	0xA1	¡
162	0xA2	¢
163	0xA3	£
164	0xA4	¤
165	0xA5	¥
166	0xA6	¦
167	0xA7	§
168	0xA8	¨
169	0xA9	©
170	0xAA	ª
171	0xAB	«
172	0xAC	¬
173	0xAD	
174	0xAE	®
175	0xAF	¯
176	0xB0	°
177	0xB1	±
178	0xB2	²

179	0xB3	³
180	0xB4	´
181	0xB5	µ
182	0xB6	¶
183	0xB7	·
184	0xB8	¸
185	0xB9	¹
186	0xBA	º
187	0xBB	»
188	0xBC	¼
189	0xBD	½
190	0xBE	¾
191	0xBF	¿
192	0xC0	À
193	0xC1	Á
194	0xC2	Â
195	0xC3	Ã
196	0xC4	Ä
197	0xC5	Å
198	0xC6	Æ
199	0xC7	Ç
200	0xC8	È
201	0xC9	É
202	0xCA	Ê
203	0xCB	Ë

204	0xCC	Ì
205	0xCD	Í
206	0xCE	Î
207	0xCF	Ï
208	0xD0	Ð
209	0xD1	Ñ
210	0xD2	Ò
211	0xD3	Ó
212	0xD4	Ô
213	0xD5	Õ
214	0xD6	Ö
215	0xD7	×
216	0xD8	Ø
217	0xD9	Ù
218	0xDA	Ú
219	0xDB	Û
220	0xDC	Ü
221	0xDD	Ý
222	0xDE	Þ
223	0xDF	ß
224	0xE0	à
225	0xE1	á
226	0xE2	â
227	0xE3	ã
228	0xE4	ä

229	0xE5	å
230	0xE6	æ
231	0xE7	ç
232	0xE8	è
233	0xE9	é
234	0xEA	ê
235	0xEB	ë
236	0xEC	ì
237	0xED	í
238	0xEE	î
239	0xEF	ï
240	0xF0	ð
241	0xF1	ñ
242	0xF2	ò
243	0xF3	ó
244	0xF4	ô
245	0xF5	õ
246	0xF6	ö
247	0xF7	÷
248	0xF8	ø
249	0xF9	ù
250	0xFA	ú
251	0xFB	û
252	0xFC	ü
253	0xFD	ý

254	0xFE	þ
255	0xFF	ÿ